UNIVERSIDADE FEDERAL DO PARANÁ

EDSON MINORU SASSAKI

Descrição dos Objetos Galois sobre uma Álgebra de Hopf Associada a um Conjunto de Dados de Grupo

CURITIBA
2014

EDSON MINORU SASSAKI

Descrição dos Objetos Galois sobre uma Álgebra de Hopf Associada a um Conjunto de Dados de Grupo

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre em Matemática, no Curso de Pós-Graduação em Matemática, Setor de Ciências Exatas, da Universidade Federal do Paraná.

Orientador: Prof. Dr. Marcelo Muniz Silva Alves

CURITIBA
2014

Ministério da Educação
Universidade Federal do Paraná
Setor de Ciências Exatas/Departamento de Matemática
Programa de Pós-Graduação em Matemática Aplicada - PPGMA

ATA DA 61ª DEFESA DE DISSERTAÇÃO DE MESTRADO

Aos vinte e sete dias do mês de fevereiro de 2014, no Anfiteatro B, Bloco das PCs, foi instalada pelo Professor Marcelo Muniz Silva Alves, a Banca Examinadora para a sexagésima primeira Defesa de Dissertação de Mestrado em Matemática Aplicada. Estiveram presentes ao Ato, professores, alunos e visitantes.

A banca examinadora, homologada pelo Colegiado do Programa de Pós-Graduação em Matemática Aplicada, ficou constituída pelos professores: Prof. Dr. Eliezer Batista, da Universidade Federal de Santa Catarina, Profa. Dra. Paula Olga Gneri, da Universidade Tecnológica Federal do Paraná, e o Prof. Dr. Marcelo Muniz Silva Alves, orientador da dissertação, a quem coube a presidência dos trabalhos.

Às quatorze horas, a banca iniciou seus trabalhos, convidando o candidato **EDSON MINORU SASSAKI** a fazer a apresentação do tema da dissertação intitulada "DESCRIÇÃO DOS OBJETOS GALOIS SOBRE UMA ÁLGEBRA DE HOPF ASSOCIADA A UM CONJUNTO DE DADOS DE GRUPO". Encerrada a apresentação, iniciou-se a fase de argüição pelos membros participantes. Após a argüição, a banca com pelo menos 03 (três) membros, reuniu-se para apreciação do desempenho do pós-graduando.

A banca considerou que o pós-graduando fez uma apresentação com a necessária concisão. A Dissertação apresenta contribuição à área de estudos e não foram registrados problemas fundamentais de estrutura e redação, resultando em plena e satisfatória compreensão dos objetivos pretendidos.

Tendo em vista a dissertação e a argüição, os membros presentes da banca decidiram pela sua aprovação.

Curitiba, 27 de fevereiro de 2014.

Prof. Dr. Marcelo Muniz Silva Alves
Presidente

Eliezer Batista

Prof. Dr. Eliezer Batista
Titular

Paula Olga Gneri

Profa. Dra. Paula Olga Gneri
Titular

TERMO DE APROVAÇÃO

"DESCRIÇÃO DOS OBJETOS GALOIS SOBRE UMA ÁLGEBRA DE HOPF ASSOCIADA A UM CONJUNTO DE DADOS DE GRUPO"

por

EDSON MINORU SASSAKI

Dissertação aprovada como requisito parcial para obtenção do grau de Mestre no Programa de Pós-Graduação em Matemática Aplicada, pela Comissão Examinadora composta por:

Orientador: ______________________________
Prof. Dr. Marcelo Muniz silva Alves
Dep. de Matemática – UFPR

Eliezer Batista
____
Prof. Dr. Eliezer Batista
Dep. de Matemática – UFSC

Paula Olga Gneri
____
Profa. Dra. Paula Olga Gneri
Dep. de Matemática – UTFPR

Curitiba, 27 de fevereiro de 2014.

RESUMO

Neste trabalho, apresentaremos uma forma de classificar todos os objetos Galois sobre uma álgebra de Hopf associada a um conjunto de dados de grupo. Estas álgebras são introduzidas por Chen, Huang, Ye e Zhang, em seu artigo "Monomial Hopf Algebras", no qual as relacionam com álgebras de Hopf monomiais não semi simples. A classificação foi proposta por Julien Bichon, em seu artigo "Galois and Bigalois Objects Over Monomial Non-Semisimple Hopf Algebras". Além disso, damos uma caracterização de objetos Galois sobre uma álgebra de Hopf fielmente planos sobre $\mathbb{K}$ através de funtores monoidais exatos aditivos. Conceitos, como estrutura de coálgebras, comódulos, funtores aditivos exatos, biálgebras e álgebras de Hopf são apresentados para que o leitor acompanhe as demonstrações principais.

Palavras-chave: Extensão Galois, Objeto Galois, Álgebra de Hopf, Cohomologia de Grupos, Produto Cruzado

ABSTRACT

In this paper, we present a way to classify all Galois objects over a Hopf algebra associated with a group datum. These algebras were introduced by Chen, Huang, Ye and Zhang, in their article "Monomial Hopf Algebras", in which they relate them to monomial non-semisimple Hopf algebras. The classification was proposed by Julien Bichon, in his article "Galois and Bigalois Objects Over Monomial Non-Semisimple Hopf Algebras". Moreover, we give a characterization of faithfully $\mathbb{K}$-flat Galois objects over a Hopf algebra by exact additive monoidal functors. Concepts like coalgebras structure, comodules, exact additive functors, bialgebras and Hopf algebras are introduced so the reader can understand the main proofs.

Key-words: Galois Extension, Galois Object, Hopf Algebra, Group cohomology, crossed product

CONTEÚDO

INTRODUÇÃO

A menor álgebra de Hopf não comutativa e não cocomutativa foi apresentada por Sweedler no final da década de 60. Esta álgebra tem dimensão 4 sobre um corpo de característica diferente de 2 e é não semi simples. Taft generaliza esta construção em seu artigo "The Order of the Antipode of Finite-dimensional Hopf Algebra", [10], no qual apresenta uma família de álgebras de Hopf com antípoda de ordem $2d$ e dimensão d^{n+1}, onde $n \geq 1$ e $d > 1$.

As álgebras de Hopf acima são monomiais não semi simples. Estas álgebras são classificadas por Chen, Huang, Ye e Zhang, em seu artigo "Monomial Hopf Algebras", [7], no qual as descrevem como álgebras de Hopf associadas a um conjunto de dados de grupo. Um conjunto de dados de grupo é formado por um grupo finito G, um elemento g central em G, um morfismo de grupos $\chi\colon G \to \mathbb{K}^*$ e uma constante $\mu \in \mathbb{K}$ tal que se $o(g) = o(\chi(g))$, então $\mu = 0$ e se $\mu \neq 0$, então $\chi^{o(\chi(g))} = 1$. Denotamos este conjunto por $\mathbb{G} = (G, g, \chi, \mu)$ e podemos classificá-lo em 6 tipos diferentes, de modo que, se dois conjuntos de dados de grupo não são do mesmo tipo, então não podem ser isomorfos. A álgebra de Hopf associada à $\mathbb{G}$ será denotada por $A(\mathbb{G})$ e seus elementos grouplike são correpondentes aos elementos de G.

Neste trabalho, apresentaremos uma forma de classificar todos os objetos Galois e biGalois sobre uma álgebra de Hopf associada a um conjunto de dados de grupo.

Um objeto Galois (à direita) sobre uma álgebra de Hopf H é uma álgebra A que tem estrutura de H-comódulo (à direita) ρ, onde a subálgebra dos coinvariantes $A^{co\,H}$ é isomorfa à $\mathbb{K}$ e a função:

$$\kappa\colon A \otimes A \longrightarrow A \otimes H$$
$$a \otimes b \longmapsto a\rho(b)$$

é um isomorfismo de A-módulos à esquerda e de H-comódulos à direita. Um objeto biGalois sobre uma álgebra de Hopf é uma álgebra que tem a estrutura acima à esquerda e à direita, de forma compatível.

A classificação dos objetos Galois e biGalois que utilizaremos foi proposta por Julien Bichon, em seu artigo "Galois and Bigalois Objects Over Monomial Non-Semisimple Hopf Algebras", [1], onde ele estabelece relações entre estes conjuntos e versões modificadas da segunda cohomologia de grupos dos elementos grouplike.

No primeiro capítulo, conceitos, como estrutura de coálgebras, comódulos, funtores aditivos exatos, biálgebras e álgebras de Hopf são apresentados para que o leitor acompanhe as demonstrações principais. A conexão entre teoria de Galois para corpos e teoria de Galois sobre álgebras de Hopf é feita na seção 1.6, com base em "Galois Structures", [15], de Tomasz Maszczyk. Nas seções 1.3 e 1.4, desenvolvemos as ferramentas necessárias para estudarmos a estrutura de grupo do conjunto de objetos biGalois sobre uma álgebra de Hopf. que será feita na seção 1.7. Em particular, apresentamos uma correpondência bijetora entre funtores monoidais exatos que comutam com somas diretas arbitrárias ${}^{H}\mathcal{M} \to \mathcal{M}_{\mathbb{K}}$ e objetos H-Galois fielmente $\mathbb{K}$-planos.

No segundo capítulo, apresentamos a álgebra $A(\mathbb{G})$ e, para conjuntos de dados de grupo do tipo I ao tipo V, apresentamos uma família de objetos $A(\mathbb{G})$-Galois que cobre todos os outros objetos $A(\mathbb{G})$-Galois. Além disso, introduzimos uma equação que é necessária e suficiente para que um objeto seja $A(\mathbb{G})$-Galois. Esta equação será utilizada na classificação dos objetos Galois para cada tipo de conjunto de dados de grupo.

No terceiro capítulo, apresentamos uma família de objetos $A(\mathbb{G})$-biGalois que cobre todos os outros objetos $A(\mathbb{G})$-biGalois. Para os conjuntos de dados dos tipos I e II, a demonstração é feita diretamente a partir desta família. Para os tipos III e IV, precisamos também estudar objetos H-$A(\mathbb{G})$-biGalois, com H podendo ser diferente de $A(\mathbb{G})$. Os tipos V e VI são feitos a partir do caso III. Por fim, concluímos a descrição dos objetos $A(\mathbb{G})$-Galois utilizando o seguinte resultado apresentado por Schauenburg em [2]: Se H_1 e H_2 são duas álgebras de Hopf tais que existe um objeto H_1-H_2-biGalois, então temos uma bijeção entre os objetos H_1-Galois e os objetos H_2-Galois. A caracterização dos objetos $A(\mathbb{G})$-Galois para $\mathbb{G}$ do tipo VI é feita construindo um objeto $A(\mathbb{G})$-$A(\mathbb{G}')$-biGalois com $\mathbb{G}'$ do tipo III.

1. PRELIMINARES

1.1 Coálgebras e Comódulos

Nesta seção introduziremos os conceitos necessários para demonstrar o seguinte resultado e algumas de suas consequências: Sejam A um C-comódulo álgebra e I um ideal de A que é um C-subcomódulo de A. Então existe uma única estrutura de C-comódulo álgebra no quociente A/I para o qual o morfismo projeção $\pi_I \colon A \to A/I$ é morfismo de C-comódulo álgebras. Quando não houver menção contrária, $\mathbb{K}$ será um anel comutativo.

Observação 1.1. *Seja V um $\mathbb{K}$-módulo. Chamaremos de $V \colon V \to V$ o isomorfismo identidade definido por $V(x) = x$.*

Observação 1.2. *Seja V um $\mathbb{K}$-módulo. Chamaremos de $\tau_V \colon V \to V \otimes \mathbb{K}$ o isomorfismo canônico definido por $\tau_V(x) = x \otimes 1$.*

Definição 1.3. *Sejam C um $\mathbb{K}$-módulo, $\Delta_C \colon C \to C \otimes C$ e $\varepsilon_C \colon C \to \mathbb{K}$ morfismos $\mathbb{K}$-lineares. Dizemos que a tripla $(C, \Delta_C, \varepsilon_C)$ é uma coálgebra se os seguintes diagramas comutam:*

$$\begin{tikzcd}
C \arrow[r, "\Delta_C"] \arrow[d, "\Delta_C"'] & C \otimes C \arrow[d, "C\otimes\Delta_C"] \\
C \otimes C \arrow[r, "\Delta_C\otimes C"] & C \otimes C \otimes C
\end{tikzcd}$$

$$\begin{tikzcd}
& C \arrow[dl, "\cong"'] \arrow[dr, "\cong"] \arrow[dd, "\Delta_C"] & \\
\mathbb{K} \otimes C & & C \otimes \mathbb{K} \\
& C \otimes C \arrow[ul, "\varepsilon_C\otimes C"] \arrow[ur, "C\otimes\varepsilon_C"'] &
\end{tikzcd}$$

Quando não houver ambiguidade, diremos apenas que C é coálgebra.

Definição 1.4. *Sejam C e D coálgebras e $f \colon C \to D$ um morfismo $\mathbb{K}$-linear. Diremos que f é um morfismo de coálgebras se os seguintes diagramas comutam:*

$$\begin{tikzcd}
C \arrow[r, "f"] \arrow[d, "\Delta_C"'] & D \arrow[d, "\Delta_D"] \\
C \otimes C \arrow[r, "f\otimes f"] & D \otimes D
\end{tikzcd}$$

$$\begin{tikzcd}
C \arrow[rr, "f"] \arrow[dr, "\varepsilon_C"'] & & D \arrow[dl, "\varepsilon_D"] \\
& \mathbb{K} &
\end{tikzcd}$$

Notação de Sweedler: Se C é uma coálgebra, então para cada $c \in C$ denotaremos:

$$\Delta_C(c) = \sum c_1 \otimes c_2$$

Como temos que $(\Delta_C \otimes C) \circ \Delta_C = (C \otimes \Delta_C) \circ \Delta_C$, podemos extender esta notação da seguinte forma:

$$\sum c_1 \otimes c_2 \otimes c_3 := \sum c_{1,1} \otimes c_{1,2} \otimes c_2 = \sum c_1 \otimes c_{2,1} \otimes c_{2,2}$$

Esta notação será amplamente utilizada a partir da Seção 1.8.

Definição 1.5. *Sejam C uma coálgebra, M um $\mathbb{K}$-módulo e $\rho_M\colon M \to M \otimes C$ um morfismo $\mathbb{K}$-linear. Diremos que o par (M, ρ_M) é um C-comódulo à direita se os seguintes diagramas comutam:*

$$\begin{tikzcd} M \arrow[r, "\rho_M"] \arrow[d, "\rho_M"'] & M \otimes C \arrow[d, "\rho_M \otimes C"] \\ M \otimes C \arrow[r, "M \otimes \Delta_C"] & M \otimes C \otimes C \end{tikzcd}$$

$$\begin{tikzcd} M \arrow[rr, "\rho_M"] \arrow[dr, "\cong"'] & & M \otimes C \arrow[dl, "M \otimes \varepsilon_C"] \\ & M \otimes \mathbb{K} & \end{tikzcd}$$

Quando não houver ambiguidade, diremos apenas que M é C-comódulo à direita.

Definição 1.6. *Sejam C uma coálgebra, M um $\mathbb{K}$-módulo e $\beta_M\colon M \to C \otimes M$ um morfismo $\mathbb{K}$-linear. Diremos que o par (M, β_M) é um C-comódulo à esquerda se os seguintes diagramas comutam:*

$$\begin{tikzcd} M \arrow[r, "\beta_M"] \arrow[d, "\beta_M"'] & C \otimes M \arrow[d, "C \otimes \beta_M"] \\ C \otimes M \arrow[r, "\Delta_C \otimes M"] & C \otimes C \otimes M \end{tikzcd}$$

$$\begin{tikzcd} M \arrow[rr, "\beta_M"] \arrow[dr, "\cong"'] & & C \otimes M \arrow[dl, "\varepsilon_C \otimes M"] \\ & \mathbb{K} \otimes M & \end{tikzcd}$$

Quando não houver ambiguidade, diremos apenas que M é C-comódulo à esquerda.

Notação de Sweedler:

- Se (M, ρ_M) é um C-comódulo à direita, então para cada $m \in M$ denotaremos:

$$\rho_M(m) = \sum m_{(0)} \otimes m_{(1)}$$

  Como temos que $(\rho_M \otimes C) \circ \rho_M = (M \otimes \Delta_C) \circ \rho_M$, podemos extender esta notação da seguinte forma:

$$\sum m_{(0)} \otimes m_{(1)} \otimes m_{(2)} := \sum m_{(0),(0)} \otimes m_{(0),(1)} \otimes m_{(1)} = \sum m_{(0)} \otimes m_{(1),1} \otimes m_{(1),2}$$

- Se (M, β_M) é um C-comódulo à esquerda, então para cada $m \in M$ denotaremos:

$$\beta_M(m) = \sum m_{(-1)} \otimes m_{(0)}$$

  Como temos que $(C \otimes \beta_M) \circ \beta_M = (\Delta_C \otimes \beta_M) \circ \beta_M$, podemos extender esta notação da seguinte forma:

$$\sum m_{(-2)} \otimes m_{(-1)} \otimes m_{(0)} = \sum m_{(-1)} \otimes m_{(0),(-1)} \otimes m_{(0),(0)} = \sum m_{(-1),1} \otimes m_{(-1),2} \otimes m_{(0)}$$

Esta notação será utilizada na Seção 1.5.

Os próximos resultados serão feitos para C-comódulos à direita, mas possuem resultados análogos para C-comódulos à esquerda. Ocultaremos o termo "à direita", pois não há ambiguidade.

Definição 1.7. *Sejam (M, ρ_M) e (N, ρ_N) dois C-comódulos, e $f: M \to N$ um morfismo $\mathbb{K}$-linear. Diremos que f é morfismo de C-comódulos se o seguinte diagrama comuta:*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\rho_M"'] & N \arrow[d, "\rho_N"] \\ M \otimes C \arrow[r, "f \otimes C"] & N \otimes C \end{tikzcd}$$

Definição 1.8. *Seja (A, ρ_A) um C-comódulo tal que A é uma álgebra. Diremos que A é um C-comódulo álgebra se ρ_A é morfismo de álgebras. Neste caso, chamaremos ρ_A de uma coação de C sobre A.*

Definição 1.9. *Sejam A e B dois C-comódulo álgebras. Diremos que um morfismo $f: A \to B$ é um morfismo de C-comódulo álgebras se f é morfismo de álgebras e morfismo de C-comódulos.*

Teorema 1.10. *Sejam M um C-comódulo e L a álgebra tensorial sobre M. Então existe uma única estrutura de C-comódulo tal que L é C-comódulo álgebra e o morfismo inclusão $\iota: M \to L$ é morfismo de C-comódulos.*

Demonstração. Pela definição de álgebra tensorial, existe um único morfismo de álgebras ρ_L tal que o seguinte diagrama comuta:

$$\begin{tikzcd} & L \arrow[d, dotted, "\rho_L"] \\ M \arrow[ur, "\iota"] \arrow[r, "(\iota \otimes C) \circ \rho_M"'] & L \otimes C \end{tikzcd}$$

Note que, se M e L são C-comódulos, então ι é morfismo de C-comódulos pela comutatividade do diagrama acima.

Vejamos que de fato ρ_L é uma coação de C sobre L:

$$\begin{aligned}
(\rho_L \otimes C) \circ \rho_L \circ \iota &= (\rho_L \otimes C) \circ (\iota \otimes C) \circ \rho_M \\
&= \big((\rho_L \circ \iota) \otimes C\big) \circ \rho_M \\
&= \Big(\big((\iota \otimes C) \circ \rho_M\big) \otimes C\Big) \circ \rho_M \\
&= (\iota \otimes C \otimes C) \circ (\rho_M \otimes C) \circ \rho_M \\
&= (\iota \otimes C \otimes C) \circ (M \otimes \Delta_C) \circ \rho_M \\
&= (\iota \otimes \Delta_C) \circ \rho_M \\
&= (L \otimes \Delta_C) \circ (\iota \otimes C) \circ \rho_M \\
&= (L \otimes \Delta_C) \circ \rho_L \circ \iota
\end{aligned}$$

Logo, $(\rho_L \otimes C) \circ \rho_L$ e $(L \otimes \Delta_C) \circ \rho_L$ fazem o seguinte diagrama comutar:

$$\begin{tikzcd} & L \arrow[d, dotted] \\ M \arrow[ur, "\iota"] \arrow[r, "(\iota \otimes \Delta_C) \circ \rho_M"'] & L \otimes C \otimes C \end{tikzcd}$$

Pela definição de álgebra tensorial, temos que $(\rho_L \otimes C) \circ \rho_L = (L \otimes \Delta_C) \circ \rho_L$.

Do mesmo modo, temos:

$$\begin{aligned}(L\otimes\varepsilon_C)\circ\rho_L\circ\iota &= (L\otimes\varepsilon_C)\circ(\iota\otimes C)\circ\rho_M\\ &= (\iota\otimes\varepsilon_C)\circ\rho_M\\ &= (\iota\otimes\mathbb{K})\circ(M\otimes\varepsilon_C)\circ\rho_M\\ &= (\iota\otimes\mathbb{K})\circ\tau_M\\ &= \tau_L\circ\iota\end{aligned}$$

Logo, $(L\otimes\varepsilon_C)\circ\rho_L$ e τ_L fazem o seguinte diagrama comutar:

$$\begin{tikzcd} & L \arrow[d, dotted] \\ M \arrow[ur, "\iota"] \arrow[r, "(\iota\otimes\mathbb{K})\circ\tau_M"'] & L\otimes\mathbb{K}\end{tikzcd}$$

Pela definição de álgebra tensorial, temos que $(L\otimes\varepsilon_C)\circ\rho_L=\tau_L$.
Portanto L é C-comódulo álgebra e ι é morfismo de C-comódulos. □

Corolário 1.11. *Sejam M um C-comódulo, A um C-comódulo álgebra, L a álgebra tensorial sobre M e $f\colon M\to A$ um morfismo de C-comódulos. Então existe um único morfismo de C-comódulo álgebras $f'\colon L\to A$ tal que o seguinte diagrama comuta:*

$$\begin{tikzcd} & L \arrow[d, dotted, "f'"] \\ M \arrow[ur, "\iota"] \arrow[r, "f"'] & A\end{tikzcd}$$

Demonstração. Pela definição de álgebra tensorial, existe um único morfismo de álgebras f' que faz o seguinte diagrama comutar:

$$\begin{tikzcd} & L \arrow[d, dotted, "f'"] \\ M \arrow[ur, "\iota"] \arrow[r, "f"'] & A\end{tikzcd}$$

Seja ρ_L a coação de C sobre L dada pelo Teorema 1.10.
Temos que:

$$\begin{aligned}\rho_A\circ f'\circ\iota &= \rho_A\circ f\\ &= (f\otimes C)\circ\rho_M\\ &= \big((g\circ\iota)\otimes C\big)\circ\rho_M\\ &= (f'\otimes C)\circ(\iota\otimes C)\circ\rho_M\\ &= (f'\otimes C)\circ\rho_L\circ\iota\end{aligned}$$

Logo, $\rho_A\circ f'$ e $(f'\otimes C)\circ\rho_L$ fazem o seguinte diagrama comutar:

$$\begin{tikzcd} & L \arrow[d, dotted] \\ M \arrow[ur, "\iota"] \arrow[r, "((f\otimes C)\circ\rho_M"'] & A\otimes C\end{tikzcd}$$

Pela definição de álgebra tensorial, temos que $\rho_A\circ f'=(f'\otimes C)\circ\rho_L$ e portanto f' é morfismo de C-comódulo álgebras. □

Definição 1.12. *Sejam M um C-comódulo e N um $\mathbb{K}$-submódulo de M. Diremos que N é um C-subcomódulo de M se $\rho_M(N)\subset N\otimes C$.*

Neste caso, (N, ρ_N) é C-comódulo, onde $\rho_N \colon N \to N \otimes C$ é a restrição de ρ_M à N e $N \otimes C$. Além disso, o morfismo inclusão $\iota_N \colon N \to M$, $\iota_N(n) = n$, $\forall n \in N$ é morfismo de C-comódulos.

Proposição 1.13. *Sejam M um C-comódulo e N um C-subcomódulo de M. Então existe uma única estrutura de C-comódulo no quociente M/N para o qual o morfismo projeção $\pi_N \colon M \to M/N$ é morfismo de C-comódulos.*

Demonstração. Como $(\pi_N \otimes C) \circ \rho_M(N) \subset (\pi_N \otimes C)(N \otimes C) = \pi_N(N) \otimes C = 0$, pela propriedade universal de quociente de espaços, existe um único morfismo de $\mathbb{K}$-módulos $\bar{\rho}_M \colon M/N \to M/N \otimes C$ tal que o seguinte diagrama comuta:

$$\begin{tikzcd} M \arrow[rr, "(\pi_N \otimes C)\circ\rho_M"] \arrow[dr, "\pi_N"'] & & M/N \otimes C \\ & M/N \arrow[ur, dotted, "\bar{\rho}_M"'] & \end{tikzcd}$$

Note que, se M e M/N são C-comódulos, então π_N é morfismo de C-comódulos pela comutatividade do diagrama acima, pois o mesmo pode ser reescrito da seguinte forma:

$$\begin{tikzcd} M \arrow[r, "\pi_N"] \arrow[d, "\rho_M"'] & M/N \arrow[d, "\bar{\rho}_M"] \\ M \otimes C \arrow[r, "\pi_N \otimes C"] & M/N \otimes C \end{tikzcd}$$

Temos que:

$$\begin{aligned}
(\bar{\rho}_M \otimes C) \circ \bar{\rho}_M \circ \pi_N &= (\bar{\rho}_M \otimes C) \circ (\pi_N \otimes C) \circ \rho_M \\
&= ((\bar{\rho}_M \circ \pi_N) \otimes C) \circ \rho_M \\
&= (((\pi_N \otimes C) \circ \rho_M) \otimes C) \circ \rho_M \\
&= (\pi_N \otimes C \otimes C) \circ (\rho_M \otimes C) \circ \rho_M \\
&= (\pi_N \otimes C \otimes C) \circ (M \otimes \Delta_C) \circ \rho_M \\
&= (\pi_N \otimes \Delta_C) \circ \rho_M \\
&= (M/N \otimes \Delta_C) \circ (\pi_N \otimes C) \circ \rho_M \\
&= (M/N \otimes \Delta_C) \circ \bar{\rho}_M \circ \pi_N
\end{aligned}$$

e

$$\begin{aligned}
(M/N \otimes \varepsilon_C) \circ \bar{\rho}_M \circ \pi_N &= (M/N \otimes \varepsilon_C) \circ (\pi_N \otimes C) \circ \rho_M \\
&= (\pi_N \otimes \varepsilon_C) \circ \rho_M \\
&= (\pi_N \otimes \mathbb{K}) \circ (M \otimes \varepsilon_C) \circ \rho_M \\
&= (\pi_N \otimes \mathbb{K}) \circ \tau_M \\
&= \tau_{M/N} \circ \pi_N
\end{aligned}$$

Como π_N é epimorfismo, temos que:

$$(\bar{\rho}_M \otimes C) \circ \bar{\rho}_M = (M/N \otimes \Delta_C) \circ \bar{\rho}_M$$

e

$$(M/N \otimes \varepsilon_C) \circ \bar{\rho}_M = \tau_{M/N}$$

Portanto $(M/N, \bar{\rho}_M)$ é C-comódulo e π_N é morfismo de C-comódulos.
A unicidade segue da propriedade universal do quociente de espaços. □

Apresentamos agora o resultado principal desta seção.

Corolário 1.14. *Sejam A um C-comódulo álgebra e I um ideal de A que é um C-subcomódulo de A. Então existe uma única estrutura de C-comódulo álgebra no quociente A/I para o qual o morfismo projeção $\pi_I \colon A \to A/I$ é morfismo de C-comódulo álgebras.*

Demonstração. Pela Proposição 1.13, temos que existe um único morfismo $\bar{\rho}_I \colon A/I \to A/I \otimes C$ que faz A/I ser C-comódulo com $\pi_I \colon A \to A/I$ morfismo de C-comódulos.

Como I é C-subcomódulo de A, temos que $\rho_A(I) \subset I \otimes C$, o que implica que:

$$(\pi_I \otimes C) \circ \rho_A(I) \subset (\pi_I \otimes C)(I \otimes C) = 0$$

Logo, $I \subset \ker(\pi_I \otimes C) \circ \rho_A$.

Pela Proposição B.7, temos que existe um único morfismo de álgebras $f \colon A/I \to A/I \otimes C$ tal que o seguinte diagrama comuta:

$$\begin{tikzcd} A \arrow[rr, "(\pi_I \otimes C)\circ\rho_A"] \arrow[dr, "\pi_I"'] & & A/I \otimes C \\ & A/I \arrow[ur, dotted, "f"'] & \end{tikzcd}$$

Pela unicidade do morfismo que satisfaz o diagrama para $\mathbb{K}$-módulos, temos que $\bar{\rho}_A = f$ e A/I é C-comódulo álgebra com π_I morfismo de C-comódulo álgebras. $\square$

Corolário 1.15. *Sejam A e B dois C-comódulo álgebras. Se I é um ideal de A que também é um C-subcomódulo e $f \colon A \to B$ é um morfismo de C-comódulo álgebras com $I \subset \ker f$, então existe um único morfismo de C-comódulo álgebras $g \colon A/I \to B$ tal que $f = g \circ \pi_I$.*

Demonstração. Pela Proposição B.7, existe um único morfismo de álgebras $g \colon A/I \to B$ tal que $f = g \circ \pi_I$. Precisamos apenas verificar que g é morfismo de C-comódulos. Tome a estrutura de C-comódulo de A/I dada pela Proposição 1.13.

Temos que:

$$\begin{aligned} \rho_B \circ g \circ \pi_I &= \rho_B \circ f \\ &= (f \otimes C) \circ \rho_A \\ &= \big((g \circ \pi_I) \otimes C\big) \circ \rho_A \\ &= (g \otimes C) \circ (\pi_I \otimes C) \circ \rho_A \\ &= (g \otimes C) \circ \rho_{A/I} \circ \pi_I \end{aligned}$$

Como π_I é sobrejetor, temos que $\rho_B \circ g = (g \otimes C) \circ \rho_{A/I}$ e portanto g é morfismo de C-comódulo álgebras. $\square$

1.2 Bicomódulos

Definição 1.16. *Seja M um C-comódulo à direita com estrutura ρ que também é D-comódulo à esquerda com estrutura β. Dizemos que M é um D-C-bicomódulo se o seguinte diagrama comuta:*

$$\begin{tikzcd} M \arrow[r, "\rho"] \arrow[d, "\beta"'] & M \otimes C \arrow[d, "\beta\otimes C"] \\ D \otimes M \arrow[r, "D\otimes\rho"] & D \otimes M \otimes C \end{tikzcd}$$

Definição 1.17. *Sejam M e N dois D-C-bicomódulos. Dizemos que um morfismo $f\colon M \to N$ é morfismo de D-C-bicomódulos se f é morfismo de D-comódulos à esquerda e C-comódulos à direita.*

Nesta seção apresentaremos alguns resultados sobre álgebras tensoriais e quocientes que serão utilizados no Capítulo 3, análogos aos resultados de comódulo álgebras da seção anterior.

Proposição 1.18. *Sejam M um D-C-bicomódulo e L a álgebra tensorial sobre M. Então existe uma única estrutura de D-C-bicomódulo para L tal que L é D-C-bicomódulo álgebra e o morfismo inclusão $\iota\colon M \to L$ é morfismo de D-C-bicomódulos.*

Demonstração. Sejam β e ρ as estruturas de D-comódulo à esquerda e C-comódulo à direita de M, respectivamente.

Pelo Teorema 1.10, temos que L possui uma única estrutura ρ' de C-comódulo álgebra à direita tal que ι é morfismo de C-comódulos à direita. Pelo resultado análogo à esquerda, temos que L possui uma única estrutura β' de D-comódulo álgebra à esquerda tal que ι é morfismo de D-comódulos à esquerda.

Temos que os seguintes diagramas comutam:

$$\begin{tikzcd} & L \arrow[d, "\beta'"] \\ M \arrow[ur, "\iota"] \arrow[r, "(D\otimes\iota)\circ\beta"'] & D\otimes L \end{tikzcd} \qquad \begin{tikzcd} & L \arrow[d, "\rho'"] \\ M \arrow[ur, "\iota"] \arrow[r, "(\iota\otimes C)\circ\rho"'] & L\otimes C \end{tikzcd}$$

Como M é D-C-bicomódulo, temos que $(D\otimes\rho)\circ\beta = (\beta\otimes C)\circ\rho\colon M \to D\otimes M\otimes C$. Temos:

$$\begin{aligned}
(D\otimes\rho')\circ\beta'\circ\iota &= (D\otimes\rho')\circ(D\otimes\iota)\circ\beta \\
&= (D\otimes(\rho'\circ\iota))\circ\beta \\
&= (D\otimes((\iota\otimes C)\circ\rho))\circ\beta \\
&= (D\otimes\iota\otimes C)\circ(D\otimes\rho)\circ\beta \\
&= (D\otimes\iota\otimes C)\circ(\beta\otimes C)\circ\rho \\
&= (((D\otimes\iota)\circ\beta)\otimes C)\circ\rho \\
&= ((\beta'\circ\iota)\otimes C)\circ\rho \\
&= (\beta'\otimes C)\circ(\iota\otimes C)\circ\rho \\
&= (\beta'\otimes C)\circ\rho'\circ\iota
\end{aligned}$$

Logo, denotando por f a composição $(D\otimes\iota\otimes C)\circ(D\otimes\rho)\circ\beta = (D\otimes\iota\otimes C)\circ(\beta\otimes C)\circ\rho$, os morfismos $(D\otimes\rho')\circ\beta'$ e $(\beta'\otimes C)\circ\rho'$ fazem o seguinte diagrama comutar:

$$\begin{tikzcd} & L \arrow[d, dotted] \\ M \arrow[ur, "\iota"] \arrow[r, "f"'] & D\otimes L\otimes C \end{tikzcd}$$

Pela definição de álgebra tensorial, temos que $(D\otimes\rho')\circ\beta' = (\beta'\otimes C)\circ\rho'$ e L é D-C-bicomódulo álgebra. □

Proposição 1.19. *Sejam M um D-C-bicomódulo, A um D-C-bicomódulo álgebra, L a álgebra tensorial sobre M e $f\colon M \to A$ um morfismo de D-C-bicomódulos. Então existe um único morfismo de D-C-bicomódulo álgebras $f'\colon L \to A$ tal que o seguinte diagrama comuta:*

$$\begin{tikzcd} & L \arrow[d, dotted, "f'"] \\ M \arrow[ur, "\iota"] \arrow[r, "f"'] & A \end{tikzcd}$$

Demonstração. Pelo Corolário 1.11, existe um único morfismo de C-comódulo álgebras à direita $f_1\colon L \to A$ que satisfaz o diagrama. Pelo resultado análogo à esquerda, existe um único morfismo de D-comódulo álgebras à esquerda $f_2\colon L \to A$ que satisfaz o mesmo diagrama. Pela definição de álgebra tensorial, o morfismo que satisfaz o diagrama é único, o que implica que $f_1 = f_2$, que denotaremos por f', que é um morfismo de D-C-bicomódulo álgebras. □

Proposição 1.20. *Sejam A um D-C-bicomódulo álgebra e I um ideal de A que também é um D-subcomódulo à esquerda e C-subcomódulo à direita de A. Então existe uma única estrutura de D-C-bicomódulo álgebra no espaço quociente A/I para o qual o morfismo projeção $\pi_I\colon A \to A/I$ é morfismo de D-C-bicomódulo álgebras.*

Demonstração. Sejam β e ρ as estruturas de D-comódulo à esquerda e C-comódulo à direita de A, respectivamente.

Pelo Corolário 1.14, existe uma única estrutura ρ' de C-comódulo álgebra no espaço quociente A/I tal que a projeção é morfismo de C-comódulo álgebra à direita. Pelo resultado análogo à esquerda, existe uma única estrutura β' de D-comódulo álgebra no espaço quociente A/I tal que a projeção é morfismo de D-comódulo álgebras à esquerda.

Como A é D-C-bicomódulo, temos que $(D \otimes \rho) \circ \beta = (\beta \otimes C) \circ \rho\colon A \to D \otimes A \otimes C$. Temos:

$$\begin{aligned}
(D \otimes \rho') \circ \beta' \circ \pi_I &= (D \otimes \rho') \circ (D \otimes \pi_I) \circ \beta \\
&= (D \otimes (\rho' \circ \pi_I)) \circ \beta \\
&= (D \otimes ((\pi_I \otimes C) \circ \rho)) \circ \beta \\
&= (D \otimes \pi_I \otimes C) \circ (D \otimes \rho) \circ \beta \\
&= (D \otimes \pi_I \otimes C) \circ (\beta \otimes C) \circ \rho \\
&= (((D \otimes \pi_I) \circ \beta) \otimes C) \circ \rho \\
&= ((\beta' \circ \pi_I) \otimes C) \circ \rho \\
&= (\beta' \otimes C) \circ (\pi_I \otimes C) \circ \rho \\
&= (\beta' \otimes C) \circ \rho' \circ \pi_I
\end{aligned}$$

Logo, denotando por f a composição $(D \otimes \pi_I \otimes C) \circ (D \otimes \rho) \circ \beta = (D \otimes \pi_I \otimes C) \circ (\beta \otimes C) \circ \rho$, os morfismos $(D \otimes \rho') \circ \beta'$ e $(\beta' \otimes C) \circ \rho'$ fazem o seguinte diagrama comutar:

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\pi_I"'] & & D \otimes A/I \otimes C \\
& A/I \arrow[ur, dotted] &
\end{tikzcd}$$

Pela unicidade do morfismo que satisfaz o diagrama para $\mathbb{K}$-módulos, temos que:

$$(D \otimes \rho') \circ \beta' = (\beta' \otimes C) \circ \rho'$$

e A/I é D-C-bicomódulo álgebra com π_I morfismo de D-C-bicomódulo álgebras. □

Corolário 1.21. *Sejam A e B dois D-C-bicomódulo álgebras, I um ideal de A que também é um D-subcomódulo à esquerda e C-subcomódulo à direita de A e $f\colon A \to B$ morfismo de D-C-bicomódulo álgebras com $I \subset \ker f$. Então existe um único morfismo de D-C-bicomódulo álgebras $g\colon A/I \to B$ tal que $f = g \circ \pi_I$.*

Demonstração. Pelo Corolário 1.15, existe um único morfismo de C-comódulo álgebras à direita $f_1\colon A/I \to B$ tal que $f = f_1 \circ \pi_I$. Pelo resultado análogo à esquerda, existe um único morfismo de D-comódulo álgebras à esquerda $f_2\colon A/I \to B$ tal que $f = f_2 \circ \pi_I$. Logo os morfismos f_1 e f_2 fazem o seguinte diagrama comutar:

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\pi_I"'] & & B \\
& A/I \arrow[ur, dotted] &
\end{tikzcd}$$

Pela unicidade do morfismo que satisfaz o diagrama para $\mathbb{K}$-módulos, temos que $f_1 = f_2$. Denotaremos este morfismo por g, que é um morfismo de D-C-bicomódulo álgebras. $\square$

1.3 Funtores Aditivos e Produto Tensorial

Nesta seção apresentaremos os conceitos necessários para a demonstração do seguinte resultado: Seja C uma coálgebra. Denotando por ${}^{C}\mathcal{M}$ a categoria dos C-comódulos à esquerda e por $\mathcal{M}_{\mathbb{K}}$ a categoria dos $\mathbb{K}$-módulos à direita, se $\mathcal{F}\colon {}^{C}\mathcal{M} \to \mathcal{M}_{\mathbb{K}}$ é um funtor exato aditivo que comuta com somas diretas arbitrárias, então para cada $(M, \rho) \in {}^{C}\mathcal{M}$ e $V \in \mathcal{M}_{\mathbb{K}}$, existe um isomorfismo $\mathcal{F}(M \otimes V) \cong \mathcal{F}(M) \otimes V$, onde $(M \otimes V, \rho') \in {}^{C}\mathcal{M}$ com $\rho'(m \otimes v) = \rho(m) \otimes v$, tal que:

1) é coerente, ou seja, se W é outro $\mathbb{K}$-módulo à direita, então o seguinte diagrama comuta:

$$\begin{tikzcd}
\mathcal{F}(M \otimes V \otimes W) \arrow[rr, "\cong"] \arrow[dr, "\cong"'] & & \mathcal{F}(M \otimes V) \otimes W \arrow[dl, "\cong"] \\
& \mathcal{F}(M) \otimes V \otimes W &
\end{tikzcd}$$

2) é natural em M, ou seja, se N é outro C-comódulo à esquerda e $f\colon M \to N$ é um morfismo de C-comódulos à esquerda, então o seguinte diagrama comuta:

$$\begin{tikzcd}
\mathcal{F}(M \otimes V) \arrow[r, "\cong"] \arrow[d, "\mathcal{F}(f\otimes V)"'] & \mathcal{F}(M) \otimes V \arrow[d, "\mathcal{F}(f)\otimes V"] \\
\mathcal{F}(N \otimes V) \arrow[r, "\cong"] & \mathcal{F}(N) \otimes V
\end{tikzcd}$$

3) é natural em V, ou seja, se W é outro $\mathbb{K}$-módulo à direita e $f\colon V \to W$ é um morfismo de $\mathbb{K}$-módulos à direita, então o seguinte diagrama comuta:

$$\begin{tikzcd}
\mathcal{F}(M \otimes V) \arrow[r, "\cong"] \arrow[d, "\mathcal{F}(M\otimes f)"'] & \mathcal{F}(M) \otimes V \arrow[d, "\mathcal{F}(M)\otimes f"] \\
\mathcal{F}(M \otimes W) \arrow[r, "\cong"] & \mathcal{F}(M) \otimes W
\end{tikzcd}$$

Observação 1.22. *Seja $(M_i)_{i\in I}$ uma coleção em $\mathcal{M}_{\mathbb{K}}$. Denotaremos os elementos de $\bigoplus_{t\in I} M_t$ por $(m_t)_{t\in I}$, onde $m_t \in M_t$, $\forall t \in I$, com $m_t = 0$ a menos de um número finito de índices.*

Para cada $i \in I$, denotaremos por ι_i o morfismo inclusão:

$$\begin{aligned}
\iota_i\colon M_i &\longrightarrow \bigoplus_{t\in I} M_t \\
m &\longmapsto (\delta_{t,i} m)_{t\in I}
\end{aligned}$$

onde $\delta_{t,i}$ é o Delta de Kronecker e denotaremos por π_i o morfismo projeção:

$$\begin{aligned}
\pi_i\colon \bigoplus_{t\in I} M_t &\longrightarrow M_i \\
(m_t)_{t\in I} &\longmapsto m_i
\end{aligned}$$

Observação 1.23. *Se $\mathcal{F}\colon \mathcal{M}_{\mathbb{K}} \to \mathcal{M}_{\mathbb{K}}$ é um funtor, para cada $i \in I$, denotaremos por ι_i' o morfismo inclusão:*

$$\begin{aligned} \iota_i'\colon \mathcal{F}(M_i) &\longrightarrow \bigoplus_{t\in I} \mathcal{F}(M_t) \\ x &\longmapsto (\delta_{t,i}x)_{t\in I} \end{aligned}$$

e por π_i' o morfismo projeção:

$$\begin{aligned} \pi_i'\colon \bigoplus_{t\in I} \mathcal{F}(M_t) &\longrightarrow \mathcal{F}(M_i) \\ (x_t)_{t\in I} &\longmapsto x_i \end{aligned}$$

Definição 1.24. *Seja $\mathcal{F}\colon \mathcal{M}_{\mathbb{K}} \to \mathcal{M}_{\mathbb{K}}$ um funtor. Dizemos que o funtor $\mathcal{F}$ comuta com somas diretas se, para qualquer coleção $(M_i)_{i\in I}$ em $\mathcal{M}_{\mathbb{K}}$, existe um único isomorfismo:*

$$\phi_I\colon \bigoplus_{t\in I} \mathcal{F}(M_t) \to \mathcal{F}\Big(\bigoplus_{t\in I} M_t\Big)$$

que faz o seguinte diagrama comutar, para todo $i \in I$:

$$\begin{tikzcd} & \bigoplus_{t\in I} \mathcal{F}(M_t) \arrow[d, "\phi_I"] \\ \mathcal{F}(M_i) \arrow[ur, "\iota_i'"] \arrow[dr, "\mathcal{F}(\iota_i)"'] & \\ & \mathcal{F}\Big(\bigoplus_{t\in I} M_t\Big) \end{tikzcd}$$

Proposição 1.25. *Sejam $\mathcal{F}\colon \mathcal{M}_{\mathbb{K}} \to \mathcal{M}_{\mathbb{K}}$ um funtor que comuta com somas diretas e $(V_i)_{i\in I}$ uma coleção em $\mathcal{M}_{\mathbb{K}}$. Se $\phi_I\colon \bigoplus_{t\in I} \mathcal{F}(V_t) \to \mathcal{F}\Big(\bigoplus_{t\in I} V_t\Big)$ é o isomorfismo dado pela Definição 1.24, então para cada $j \in I$ o seguinte diagrama comuta:*

$$\begin{tikzcd} \bigoplus_{t\in I} \mathcal{F}(V_t) \arrow[d, "\phi_I"'] \arrow[dr, "\pi_j'"] & \\ & \mathcal{F}(V_j) \\ \mathcal{F}\Big(\bigoplus_{t\in I} V_t\Big) \arrow[ur, "\mathcal{F}(\pi_j)"'] & \end{tikzcd}$$

Demonstração. Queremos que $\mathcal{F}(\pi_j) \circ \phi_I = \pi_j', \forall j \in I$.

Para cada $i, j \in I$, temos:

- se $i \neq j$, então:

$$\begin{aligned} \pi_j' \circ \iota_i' &= 0 \\ &= \mathcal{F}(\pi_j \circ \iota_i) \\ &= \mathcal{F}(\pi_j) \circ \mathcal{F}(\iota_i) \end{aligned}$$

- se $i = j$, então:

$$\begin{aligned} \pi_i' \circ \iota_i' &= \mathcal{F}(V_i) \\ &= \mathcal{F}(\pi_i \circ \iota_i) \\ &= \mathcal{F}(\pi_i) \circ \mathcal{F}(\iota_i) \end{aligned}$$

Então, para todo $i, j \in I$, temos:

$$\begin{aligned}\mathcal{F}(\pi_j) \circ \phi_I \circ \iota_i &= \mathcal{F}(\pi_j) \circ \mathcal{F}(\iota_i) \\ &= \pi'_j \circ \iota'_i\end{aligned}$$

Para cada $j \in I$, tomando $f_i = \mathcal{F}(\pi_j) \circ \mathcal{F}(\iota_i)$, temos que $\mathcal{F}(\pi_j) \circ \phi_I$ e π'_j satisfazem o seguinte diagrama comutativo para todo $i \in I$:

$$\begin{tikzcd} & \bigoplus\limits_{t\in I} \mathcal{F}(V_t) \arrow[d, dotted] \\ \mathcal{F}(V_i) \arrow[ur, "\iota'_i"] \arrow[r, "f_i"'] & \mathcal{F}(V_j) \end{tikzcd}$$

Pela definição de soma direta, o morfismo que satisfaz este diagrama é único. Portanto $\mathcal{F}(\pi_j) \circ \phi_I = \pi'_j$, $\forall j \in I$. □

Observação 1.26. *Seja $(V, \beta) \in {}^C\mathcal{M}$ e I um conjunto não-vazio. Denotaremos por $V^{(I)}$ a soma direta $\bigoplus\limits_{i\in I} V_i$ com $V_i = V$, $\forall i \in I$.*

Então $(V^{(I)}, \beta_{(I)})$ é C-comódulo com estrutura dada pela composição:

$$V^{(I)} \xrightarrow{\beta^{(I)}} (C \otimes V)^{(I)} \xrightarrow{\cong} C \otimes (V^{(I)})$$

ou seja:

$$\beta_{(I)}((v_t)_{t\in I}) = \sum v_{t,(-1)} \otimes (v_{t,(0)})_{t\in I}$$

Observação 1.27. *Seja $V \in \mathcal{M}_{\mathbb{K}}$. Se $(a_{j,i})_{i\in I, j\in J}$ é uma matriz, chamamos de $(a_{J,I})$ o morfismo:*

$$\begin{aligned}(a_{J,I})\colon V^{(I)} &\longrightarrow V^{(J)} \\ (v_t)_{t\in I} &\longmapsto \Big(\sum_{i\in I} a_{j,i} v_i\Big)_{j\in J}\end{aligned}$$

Claramente se $V \in {}^C\mathcal{M}$, então $(a_{J,I})$ é morfismo de C-comódulos.

Observação 1.28. *Seja $V \in \mathcal{M}_{\mathbb{K}}$. Chamaremos de φ_I o isomorfismo:*

$$\begin{aligned}\varphi_I\colon V \otimes \mathbb{K}^{(I)} &\longrightarrow V^{(I)} \\ v \otimes (\lambda_t)_{t\in I} &\longmapsto (\lambda_t v)_{t\in I}\end{aligned}$$

Claramente se $V \in {}^C\mathcal{M}$, então φ_I é isomorfismo de C-comódulos.

Lema 1.29. *Sejam $V \in \mathcal{M}_{\mathbb{K}}$ e $W \in {}^C\mathcal{M}$. Dada uma resolução projetiva de V:*

$$\mathbb{K}^{(I)} \xrightarrow{(a_{J,I})} \mathbb{K}^{(J)} \xrightarrow{q} V \longrightarrow 0$$

existe um morfismo $q'\colon W^{(J)} \to W \otimes V$ de C-comódulos à esquerda tal que a seguinte sequência é exata:

$$W^{(I)} \xrightarrow{(a_{J,I})} W^{(J)} \xrightarrow{q'} W \otimes V \longrightarrow 0$$

Além disso, se $Z \in {}^C\mathcal{M}$ e $f\colon W \to Z$ é um morfismo de C-comódulos, o seguinte diagrama comuta:

$$\begin{tikzcd} W^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "f^{(I)}"'] & W^{(J)} \arrow[r, "q'"] \arrow[d, "f^{(J)}"] & W \otimes V \arrow[r] \arrow[d, "f\otimes V"] & 0 \\ Z^{(I)} \arrow[r, "(a_{J,I})"] & Z^{(J)} \arrow[r, "q''"] & Z \otimes V \arrow[r] & 0 \end{tikzcd}$$

Demonstração. Como o funtor $(W \otimes \_)$ é exato à direita, temos a seguinte sequência exata:

$$W \otimes \mathbb{K}^{(I)} \xrightarrow{W\otimes(a_{J,I})} W \otimes \mathbb{K}^{(J)} \xrightarrow{W\otimes q} W \otimes V \longrightarrow 0$$

Tome $p' = \varphi_J \circ (W \otimes (a_{J,I})) \circ \varphi_I^{-1}$ e $q' = (W \otimes q) \circ \varphi_J^{-1}$. Então o seguinte diagrama comuta:

$$\begin{tikzcd}
W \otimes \mathbb{K}^{(I)} \arrow[r, "W\otimes(a_{J,I})"] \arrow[d, "\varphi_I"'] & W \otimes \mathbb{K}^{(J)} \arrow[r, "W\otimes q"] \arrow[d, "\varphi_J"] & W \otimes V \arrow[r] \arrow[d, equal] & 0 \\
W^{(I)} \arrow[r, "p'"] & W^{(J)} \arrow[r, "q'"] & W \otimes V \arrow[r] & 0
\end{tikzcd}$$

Note que, para cada $i \in I$, temos:

$$\begin{aligned}
p'\big((\delta_{t,i}w)_{t\in I}\big) &= \varphi_J \circ (W \otimes (a_{J,I})) \circ \varphi_I^{-1}\big((\delta_{t,i}w)_{t\in I}\big) \\
&= \varphi_J \circ (W \otimes (a_{J,I}))(w \otimes (\delta_{t,i})_{t\in I}) \\
&= \varphi_J\Big(w \otimes \big(\sum_{t\in I} a_{j,i}\, \delta_{t,i}\big)_{j\in J}\Big) \\
&= \Big(\sum_{t\in I} a_{j,i}\, \delta_{t,i} w\Big)_{j\in J}
\end{aligned}$$

Portanto $p' = (a_{J,I})$ e a seguinte sequência é exata:

$$W^{(I)} \xrightarrow{(a_{J,I})} W^{(J)} \xrightarrow{q'} W \otimes V \longrightarrow 0$$

Além disso, p' e q' são morfismos de C-comódulos, pois $(a_{J,I})$, $(W \otimes q)$ e φ_J^{-1} são morfismos de C-comódulos.

Seja $Z \in {}^C\mathcal{M}$ e $f\colon W \to Z$ um morfismo. O seguinte diagrama comuta:

$$\begin{tikzcd}
W^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "f^{(I)}"'] & W^{(J)} \arrow[d, "f^{(J)}"] \\
Z^{(I)} \arrow[r, "(a_{J,I})"] & Z^{(J)}
\end{tikzcd}$$

pois, se $(w_t)_{t\in I} \in W^{(I)}$, então:

$$\begin{aligned}
f^{(J)} \circ (a_{J,I})\big((w_t)_{t\in I}\big) &= f^{(J)}\Big(\Big(\sum_{i\in I} a_{j,i} w_i\Big)_{j\in J}\Big) \\
&= \Big(f\big(\sum_{i\in I} a_{j,i} w_i\big)\Big)_{j\in J} \\
&= \Big(\sum_{i\in I} a_{j,i} f(w_i)\Big)_{j\in J} \\
&= (a_{J,I})\big((f(w_t))_{t\in I}\big) \\
&= (a_{J,I}) \circ f^{(I)}\big((w_t)_{t\in I}\big)
\end{aligned}$$

Além disso, tomando $q'' = (Z \otimes q) \circ \varphi_J^{-1}$, temos que:

$$\begin{aligned}
(f \otimes V) \circ q' &= (f \otimes V) \circ (W \otimes q) \circ \varphi_J^{-1} \\
&= (f \otimes q) \circ \varphi_J^{-1} \\
&= (Z \otimes q) \circ (f \otimes \mathbb{K}^{(J)}) \circ \varphi_J^{-1} \\
&= (Z \otimes q) \circ \varphi_J^{-1} \circ \varphi_J \circ (f \otimes \mathbb{K}^{(J)}) \circ \varphi_J^{-1} \\
&= q'' \circ f^{(J)}
\end{aligned}$$

Portanto o seguinte diagrama comuta:

$$\begin{tikzcd}
W^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "f^{(I)}"'] & W^{(J)} \arrow[r, "q'"] \arrow[d, "f^{(J)}"] & W \otimes V \arrow[r] \arrow[d, "f\otimes V"] & 0 \\
Z^{(I)} \arrow[r, "(a_{J,I})"] & Z^{(J)} \arrow[r, "q''"] & Z \otimes V \arrow[r] & 0
\end{tikzcd}$$

□

Lema 1.30. *Sejam $V, W, Z \in \mathcal{M}_{\mathbb{K}}$ e $f\colon V \to W$ um morfismo. Dadas resoluções projetivas de V e W:*

$$\begin{tikzcd}
\mathbb{K}^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "(c_{K,I})"'] & \mathbb{K}^{(J)} \arrow[r, "q_1"] \arrow[d, "(d_{L,J})"] & V \arrow[r] \arrow[d, "f"] & 0 \\
\mathbb{K}^{(K)} \arrow[r, "(b_{L,K})"] & \mathbb{K}^{(L)} \arrow[r, "q_2"] & W \arrow[r] & 0
\end{tikzcd}$$

onde os morfismos $(c_{K,I})\colon \mathbb{K}^{(I)} \to \mathbb{K}^{(K)}$ e $(d_{L,J})\colon \mathbb{K}^{(J)} \to \mathbb{K}^{(L)}$ são dados pelo teorema da comparação para resoluções projetivas, temos que o seguinte diagrama comuta:

$$\begin{tikzcd}
Z^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "(c_{K,I})"'] & Z^{(J)} \arrow[r, "q_1'"] \arrow[d, "(d_{L,J})"] & Z \otimes V \arrow[r] \arrow[d, "Z\otimes f"] & 0 \\
Z^{(K)} \arrow[r, "(b_{L,K})"] & Z^{(L)} \arrow[r, "q_2'"] & Z \otimes W \arrow[r] & 0
\end{tikzcd}$$

Demonstração. Pelo Lema 1.29, as linhas são exatas. O diagrama:

$$\begin{tikzcd}
Z^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "(c_{K,I})"'] & Z^{(J)} \arrow[d, "(d_{L,J})"] \\
Z^{(K)} \arrow[r, "(b_{L,K})"] & Z^{(L)}
\end{tikzcd}$$

claramente comuta, pois os morfismos são análogos aos do teorema da comparação para resoluções projetivas.

Além disso, temos que:

$$\begin{aligned}
(Z \otimes f) \circ q_1' &= (Z \otimes f) \circ (Z \otimes q_1) \circ \varphi_J^{-1} \\
&= \big(Z \otimes (f \circ q_1)\big) \circ \varphi_J^{-1} \\
&= \big(Z \otimes (q_2 \circ (d_{L,J}))\big) \circ \varphi_J^{-1} \\
&= (Z \otimes q_2) \circ (Z \otimes (d_{L,J})) \circ \varphi_J^{-1} \\
&= (Z \otimes q_2) \circ \varphi_L^{-1} \circ \varphi_L \circ (Z \otimes (d_{L,J})) \circ \varphi_J^{-1} \\
&= q_2' \circ (d_{L,J})
\end{aligned}$$

Portanto o seguinte diagrama comuta:

$$\begin{tikzcd}
Z^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "(c_{K,I})"'] & Z^{(J)} \arrow[r, "q_1'"] \arrow[d, "(d_{L,J})"] & Z \otimes V \arrow[r] \arrow[d, "Z\otimes f"] & 0 \\
Z^{(K)} \arrow[r, "(b_{L,K})"] & Z^{(L)} \arrow[r, "q_2'"] & Z \otimes W \arrow[r] & 0
\end{tikzcd}$$

□

Lema 1.31. *Sejam $V \in \mathcal{M}_{\mathbb{K}}$, $\mathcal{F}\colon \mathcal{M}_{\mathbb{K}} \to \mathcal{M}_{\mathbb{K}}$ um funtor que comuta com somas diretas e $(a_{j,i})_{i\in I, j\in J}$ uma matriz. Então o seguinte diagrama comuta:*

$$\begin{tikzcd}
\mathcal{F}(V)^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "\phi_I"'] & \mathcal{F}(V)^{(J)} \arrow[d, "\phi_J"] \\
\mathcal{F}\big(V^{(I)}\big) \arrow[r, "\mathcal{F}((a_{J,I}))"] & \mathcal{F}\big(V^{(J)}\big)
\end{tikzcd}$$

Demonstração. Como $\mathcal{F}$ comuta com somas diretas, o seguinte diagrama comuta:

$$\begin{tikzcd}
 & \mathcal{F}(V)^{(I)} \arrow[dd, "\phi_I"] \\
\mathcal{F}(V) \arrow[ur, "\iota_i'"] \arrow[dr, "\mathcal{F}(\iota_i)"'] & \\
 & \mathcal{F}\big(V^{(I)}\big)
\end{tikzcd}$$

Pela Proposição 1.25, para cada $j \in J$, o seguinte diagrama comuta:

$$\begin{tikzcd}
\mathcal{F}(V)^{(J)} \arrow[dd, "\phi_J"'] \arrow[dr, "\pi_j'"] & \\
 & \mathcal{F}(V) \\
\mathcal{F}\big(V^{(J)}\big) \arrow[ur, "\mathcal{F}(\pi_j)"'] &
\end{tikzcd}$$

Assim temos:

$$\mathcal{F}(\pi_j \circ (a_{J,I}) \circ \iota_i) = \mathcal{F}(\pi_j) \circ \mathcal{F}((a_{J,I})) \circ \mathcal{F}(\iota_i) = \pi_j' \circ \phi_J^{-1} \circ \mathcal{F}((a_{J,I})) \circ \phi_I \circ \iota_i'$$

Além disso, para cada $i \in I$ e $j \in J$ fixados, temos:

- dado $v \in V$:

$$\begin{aligned}
\pi_j \circ (a_{J,I}) \circ \iota_i(v) &= \pi_j \circ (a_{J,I})\big((\delta_{t,i}v)_{t\in I}\big) \\
&= \pi_j\Big(\Big(\sum_{k\in I} a_{r,k}\delta_{k,i}v\Big)_{r\in J}\Big) \\
&= \pi_j\big((a_{r,i}v)_{r\in J}\big) \\
&= a_{j,i}v \\
&= a_{j,i}V(v)
\end{aligned}$$

- dado $x \in \mathcal{F}(V)$:

$$\begin{aligned}
\pi_j' \circ (a_{J,I}) \circ \iota_i'(x) &= \pi_j' \circ (a_{J,I})\big((\delta_{t,i}x)_{t\in I}\big) \\
&= \pi_j'\Big(\Big(\sum_{k\in I} a_{r,k}\delta_{k,i}x\Big)_{r\in J}\Big) \\
&= \pi_j'\big((a_{r,i}x)_{r\in J}\big) \\
&= a_{j,i}x \\
&= a_{j,i}\mathcal{F}(V)(x)
\end{aligned}$$

Logo, temos:

$$\begin{aligned}
\mathcal{F}(\pi_j \circ (a_{J,I}) \circ \iota_i)(x) &= \mathcal{F}(a_{j,i}\, V)(x) \\
&= a_{j,i}\, \mathcal{F}(V)(x) \\
&= a_{j,i}\, x \\
&= \pi_j' \circ (a_{J,I}) \circ \iota_i'(x)
\end{aligned}$$

e o seguinte diagrama comuta, $\forall i \in I,\ j \in J$:

$$\begin{tikzcd}
 & \mathcal{F}(V)^{(I)} \arrow[r, "(a_{J,I})"] & \mathcal{F}(V)^{(J)} \arrow[dr, "\pi'_j"] & \\
\mathcal{F}(V) \arrow[ur, "\iota'_i"] \arrow[dr, "\mathcal{F}(\iota_i)"'] & & & \mathcal{F}(V) \\
 & \mathcal{F}\big(V^{(I)}\big) \arrow[r, "\mathcal{F}((a_{J,I}))"] & \mathcal{F}\big(V^{(J)}\big) \arrow[ur, "\mathcal{F}(\pi_j)"'] &
\end{tikzcd}$$

Assim, os morfismos $\pi'_j \circ (a_{J,I})$ e $\pi'_j \circ \phi_J^{-1} \circ \mathcal{F}((a_{J,I})) \circ \phi_I$ fazem o seguinte diagrama comutar:

$$\begin{tikzcd}
 & \mathcal{F}(V)^{(I)} \arrow[dd, dotted] \\
\mathcal{F}(V) \arrow[ur, "\iota'_i"] \arrow[dr, "\mathcal{F}(\pi_j \circ (a_{J,I}) \circ \iota_i)"'] & \\
 & \mathcal{F}(V)
\end{tikzcd}$$

Pela definição de soma direta, existe um único morfismo que faz o diagrama comutar. Portanto $\pi'_j \circ (a_{J,I}) = \pi'_j \circ \phi_J^{-1} \circ \mathcal{F}((a_{J,I})) \circ \phi_I$, $\forall j \in J$.

Como $\sum_{j \in J} \pi'_j \circ f = f$, $\forall f \colon \mathcal{F}(V)^{(I)} \to \mathcal{F}(V)^{(J)}$, temos que:

$$(a_{J,I}) = \phi_J^{-1} \circ \mathcal{F}((a_{J,I})) \circ \phi_I$$

e portanto o seguinte diagrama comuta:

$$\begin{tikzcd}
\mathcal{F}(V)^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "\phi_I"'] & \mathcal{F}(V)^{(J)} \arrow[d, "\phi_J"] \\
\mathcal{F}\big(V^{(I)}\big) \arrow[r, "\mathcal{F}((a_{J,I}))"] & \mathcal{F}\big(V^{(J)}\big)
\end{tikzcd}$$

□

Lema 1.32. *Sejam $V, W \in \mathcal{M}_{\mathbb{K}}$, $\mathcal{F} \colon \mathcal{M}_{\mathbb{K}} \to \mathcal{M}_{\mathbb{K}}$ um funtor que comuta com somas diretas e $f \colon V \to W$ um morfismo de $\mathbb{K}$-módulos. Então o seguinte diagrama comuta, para toda coleção I:*

$$\begin{tikzcd}
\mathcal{F}(V)^{(I)} \arrow[r, "\mathcal{F}(f)^{(I)}"] \arrow[d, "\phi_I"'] & \mathcal{F}(W)^{(I)} \arrow[d, "\phi_I"] \\
\mathcal{F}\big(V^{(I)}\big) \arrow[r, "\mathcal{F}(f^{(I)})"] & \mathcal{F}\big(W^{(I)}\big)
\end{tikzcd}$$

Demonstração. Como $\mathcal{F}$ comuta com somas diretas, o seguinte diagrama comuta:

$$\begin{tikzcd}
 & \mathcal{F}(V)^{(I)} \arrow[dd, "\phi_I"] \\
\mathcal{F}(V) \arrow[ur, "\iota'_i"] \arrow[dr, "\mathcal{F}(\iota_i)"'] & \\
 & \mathcal{F}\big(V^{(I)}\big)
\end{tikzcd}$$

Pela Proposição 1.25, para cada $j \in I$, o seguinte diagrama comuta:

$$\begin{tikzcd}
\mathcal{F}(W)^{(I)} \arrow[dd, "\phi_I"'] \arrow[dr, "\pi'_j"] & \\
& \mathcal{F}(W) \\
\mathcal{F}\big(W^{(I)}\big) \arrow[ur, "\mathcal{F}(\pi_j)"'] &
\end{tikzcd}$$

Assim temos:

$$\mathcal{F}(\pi_j \circ f^{(I)} \circ \iota_i) = \pi'_j \circ \phi_I^{-1} \circ \mathcal{F}(f^{(I)}) \circ \phi_I \circ \iota'_i$$

Além disso, para cada $i, j \in I$ fixados, temos:

- se $i \neq j$, então:

$$\begin{aligned}\pi'_j \circ \mathcal{F}(f)^{(I)} \circ \iota'_i &= 0 \\ &= \mathcal{F}(\pi_j \circ f^{(I)} \circ \iota_i)\end{aligned}$$

- se $i = j$, então:

$$\begin{aligned}\pi'_i \circ \mathcal{F}(f)^{(I)} \circ \iota'_i &= \mathcal{F}(f) \\ &= \mathcal{F}(\pi_i \circ f^{(I)} \circ \iota_i)\end{aligned}$$

e o seguinte diagrama comuta, $\forall i, j \in I$:

$$\begin{tikzcd}
& \mathcal{F}(V)^{(I)} \arrow[r, "\mathcal{F}(f)^{(I)}"] & \mathcal{F}(W)^{(I)} \arrow[dr, "\pi'_j"] & \\
\mathcal{F}(V) \arrow[ur, "\iota'_i"] \arrow[dr, "\mathcal{F}(\iota_i)"'] & & & \mathcal{F}(W) \\
& \mathcal{F}\big(V^{(I)}\big) \arrow[r, "\mathcal{F}(f^{(I)})"] & \mathcal{F}\big(W^{(I)}\big) \arrow[ur, "\mathcal{F}(\pi_j)"'] &
\end{tikzcd}$$

Assim, os morfismos $\pi'_j \circ f^{(I)}$ e $\pi'_j \circ \phi_I^{-1} \circ \mathcal{F}(f^{(I)}) \circ \phi_I$ fazem o seguinte diagrama comutar:

$$\begin{tikzcd}
& \mathcal{F}(V)^{(I)} \arrow[dd, dotted] \\
\mathcal{F}(V) \arrow[ur, "\iota'_i"] \arrow[dr, "\mathcal{F}(\pi_j \circ f^{(I)} \circ \iota_i)"'] & \\
& \mathcal{F}(V)
\end{tikzcd}$$

Pela definição de soma direta, existe um único morfismo que satisfaz o diagrama. Portanto $\pi'_j \circ f^{(I)} = \pi'_j \circ \phi_I^{-1} \circ \mathcal{F}(f^{(I)}) \circ \phi_I$, $\forall j \in J$.

Como $\sum_{j \in I} \pi'_j \circ f = f$, $\forall f \colon \mathcal{F}(V)^{(I)} \to \mathcal{F}(W)^{(I)}$, temos que:

$$\mathcal{F}(f)^{(I)} = \phi_I^{-1} \circ \mathcal{F}(f^{(I)}) \circ \phi_I$$

e portanto o seguinte diagrama comuta:

$$\begin{tikzcd}
\mathcal{F}(V)^{(I)} \arrow[r, "\mathcal{F}(f)^{(I)}"] \arrow[d, "\phi_I"'] & \mathcal{F}(W)^{(I)} \arrow[d, "\phi_I"] \\
\mathcal{F}\big(V^{(I)}\big) \arrow[r, "\mathcal{F}(f^{(I)})"] & \mathcal{F}\big(W^{(I)}\big)
\end{tikzcd}$$

$\square$

Agora apresentaremos o resultado principal desta seção.

Teorema 1.33. *Sejam C uma coálgebra e $\mathcal{F}\colon {}^C\mathcal{M} \to \mathcal{M}_{\mathbb{K}}$ um funtor exato aditivo que comuta com somas diretas arbitrárias. Então para cada $(M,\rho) \in {}^C\mathcal{M}$ e $V \in \mathcal{M}_{\mathbb{K}}$, existe um isomorfismo $\mathcal{F}(M\otimes V) \cong \mathcal{F}(M)\otimes V$, onde $(M\otimes V,\rho') \in {}^C\mathcal{M}$ com $\rho'(m\otimes v) = \rho(m)\otimes v$, tal que:*

1) é coerente, ou seja, se W é outro $\mathbb{K}$-módulo à direita, então o seguinte diagrama comuta:

$$\begin{tikzcd} \mathcal{F}(M\otimes V\otimes W) \arrow[rr, "\cong"] \arrow[dr, "\cong"'] & & \mathcal{F}(M\otimes V)\otimes W \arrow[dl, "\cong"] \\ & \mathcal{F}(M)\otimes V\otimes W & \end{tikzcd}$$

2) é natural em M, ou seja, se N é outro C-comódulo à esquerda e $f\colon M \to N$ é um morfismo de C-comódulos à esquerda, então o seguinte diagrama comuta:

$$\begin{tikzcd} \mathcal{F}(M\otimes V) \arrow[r, "\cong"] \arrow[d, "\mathcal{F}(f\otimes V)"'] & \mathcal{F}(M)\otimes V \arrow[d, "\mathcal{F}(f)\otimes V"] \\ \mathcal{F}(N\otimes V) \arrow[r, "\cong"] & \mathcal{F}(N)\otimes V \end{tikzcd}$$

3) é natural em V, ou seja, se W é outro $\mathbb{K}$-módulo à direita e $f\colon V \to W$ é um morfismo de $\mathbb{K}$-módulos à direita, então o seguinte diagrama comuta:

$$\begin{tikzcd} \mathcal{F}(M\otimes V) \arrow[r, "\cong"] \arrow[d, "\mathcal{F}(M\otimes f)"'] & \mathcal{F}(M)\otimes V \arrow[d, "\mathcal{F}(M)\otimes f"] \\ \mathcal{F}(M\otimes W) \arrow[r, "\cong"] & \mathcal{F}(M)\otimes W \end{tikzcd}$$

Demonstração. A coerência não será demonstrada.

Sejam $M \in {}^C\mathcal{M}$ e $V \in \mathcal{M}_{\mathbb{K}}$. Considere a seguinte resolução projetiva de V:

$$\mathbb{K}^{(I)} \xrightarrow{(a_{J,I})} \mathbb{K}^{(J)} \xrightarrow{q} V \longrightarrow 0$$

Pelo Lema 1.29, temos a seguinte sequência exata:

$$M^{(I)} \xrightarrow{(a_{J,I})} M^{(J)} \longrightarrow M\otimes V \longrightarrow 0$$

Aplicando o funtor $\mathcal{F}$, temos:

$$\mathcal{F}\big(M^{(I)}\big) \xrightarrow{\mathcal{F}((a_{J,I}))} \mathcal{F}\big(M^{(J)}\big) \longrightarrow \mathcal{F}(M\otimes V) \longrightarrow 0$$

Também pelo Lema 1.29, temos a seguinte sequência exata:

$$\mathcal{F}(M)^{(I)} \xrightarrow{(a_{J,I})} \mathcal{F}(M)^{(J)} \longrightarrow \mathcal{F}(M)\otimes V \longrightarrow 0$$

Pelo Lema 1.31, o seguinte diagrama comuta:

$$\begin{tikzcd} \mathcal{F}(M)^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "\phi_I"'] & \mathcal{F}(M)^{(J)} \arrow[d, "\phi_J"] \\ \mathcal{F}\big(M^{(I)}\big) \arrow[r, "\mathcal{F}((a_{J,I}))"] & \mathcal{F}\big(M^{(J)}\big) \end{tikzcd}$$

Logo, existe um único isomorfismo $\theta\colon \mathcal{F}(M)\otimes V \to \mathcal{F}(M\otimes V)$ que faz o seguinte diagrama comutar:

$$\begin{tikzcd} \mathcal{F}(M)^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "\phi_I"'] & \mathcal{F}(M)^{(J)} \arrow[r] \arrow[d, "\phi_J"] & \mathcal{F}(M)\otimes V \arrow[r] \arrow[d, dotted, "\theta"] & 0 \\ \mathcal{F}\big(M^{(I)}\big) \arrow[r, "\mathcal{F}((a_{J,I}))"] & \mathcal{F}\big(M^{(J)}\big) \arrow[r] & \mathcal{F}(M\otimes V) \arrow[r] & 0 \end{tikzcd}$$

- Naturalidade em V: A naturalidade em V é provada juntamente com a independência da escolha da resolução projetiva. Seja $W \in \mathcal{M}_{\mathbb{K}}$ um outro $\mathbb{K}$-módulo. Tome uma resolução projetiva de W:
$$\mathbb{K}^{(K)} \xrightarrow{(b_{L,K})} \mathbb{K}^{(L)} \longrightarrow W \longrightarrow 0$$
e $f\colon V \to W$ um morfismo de $\mathbb{K}$-módulos. Pelo teorema da comparação para resoluções projetivas, existem morfismos $(c_{K,I})\colon \mathbb{K}^{(I)} \to \mathbb{K}^{(K)}$ e $(d_{L,J})\colon \mathbb{K}^{(J)} \to \mathbb{K}^{(L)}$ que fazem o seguinte diagrama comutar:
$$\begin{tikzcd}
\mathbb{K}^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "(c_{K,I})"'] & \mathbb{K}^{(J)} \arrow[r] \arrow[d, "(d_{L,J})"] & V \arrow[r] \arrow[d, "f"] & 0 \\
\mathbb{K}^{(K)} \arrow[r, "(b_{L,K})"] & \mathbb{K}^{(L)} \arrow[r] & W \arrow[r] & 0
\end{tikzcd}$$
Pelo Lema 1.30, os seguintes diagramas comutam:
$$\begin{tikzcd}
M^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "(c_{K,I})"'] & M^{(J)} \arrow[r] \arrow[d, "(d_{L,J})"] & M \otimes V \arrow[r] \arrow[d, "M\otimes f"] & 0 \\
M^{(K)} \arrow[r, "(b_{L,K})"] & M^{(L)} \arrow[r] & M \otimes W \arrow[r] & 0
\end{tikzcd}$$
$$\begin{tikzcd}
\mathcal{F}(M)^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "(c_{K,I})"'] & \mathcal{F}(M)^{(J)} \arrow[r] \arrow[d, "(d_{L,J})"] & \mathcal{F}(M) \otimes V \arrow[r] \arrow[d, "\mathcal{F}(M)\otimes f"] & 0 \\
\mathcal{F}(M)^{(K)} \arrow[r, "(b_{L,K})"] & \mathcal{F}(M)^{(L)} \arrow[r] & \mathcal{F}(M) \otimes W \arrow[r] & 0
\end{tikzcd}$$
Pelo Lema 1.31, os seguintes diagramas comutam:
$$\begin{tikzcd}
\mathcal{F}(M)^{(I)} \arrow[r, "(c_{K,I})"] \arrow[d, "\phi_I"'] & \mathcal{F}(M)^{(K)} \arrow[d, "\phi_K"] \\
\mathcal{F}\big(M^{(I)}\big) \arrow[r, "\mathcal{F}((c_{K,I}))"] & \mathcal{F}\big(M^{(K)}\big)
\end{tikzcd}$$
$$\begin{tikzcd}
\mathcal{F}(M)^{(J)} \arrow[r, "(d_{L,J})"] \arrow[d, "\phi_J"'] & \mathcal{F}(M)^{(L)} \arrow[d, "\phi_L"] \\
\mathcal{F}\big(M^{(J)}\big) \arrow[r, "\mathcal{F}((d_{L,J}))"] & \mathcal{F}\big(M^{(L)}\big)
\end{tikzcd}$$
Portanto o seguinte diagrama comuta:
$$\begin{tikzcd}
\mathcal{F}(M)^{(I)} \arrow[rr, "(a_{J,I})"] \arrow[dr, "(c_{K,I})"] \arrow[dd, "\phi_I"'] & & \mathcal{F}(M)^{(J)} \arrow[rr] \arrow[dr, "(d_{L,J})"] \arrow[dd, "\phi_J"] & & \mathcal{F}(M) \otimes V \arrow[rr] \arrow[dr, "\mathcal{F}(M)\otimes f"] \arrow[dd, "\theta_V"] & & 0 & \\
& \mathcal{F}(M)^{(K)} \arrow[rr, "(b_{L,K})"] \arrow[dd, "\phi_K"] & & \mathcal{F}(M)^{(L)} \arrow[rr] \arrow[dd, "\phi_L"] & & \mathcal{F}(M) \otimes W \arrow[rr] \arrow[dd, "\theta_W"] & & 0 \\
\mathcal{F}\big(M^{(I)}\big) \arrow[rr, "\mathcal{F}((a_{J,I}))"] \arrow[dr, "\mathcal{F}((c_{K,I}))"'] & & \mathcal{F}\big(M^{(J)}\big) \arrow[rr] \arrow[dr, "\mathcal{F}((d_{L,J}))"'] & & \mathcal{F}(M \otimes V) \arrow[rr] \arrow[dr, "\mathcal{F}(M\otimes f)"'] & & 0 & \\
& \mathcal{F}\big(M^{(K)}\big) \arrow[rr, "\mathcal{F}((b_{L,K}))"] & & \mathcal{F}\big(M^{(L)}\big) \arrow[rr] & & \mathcal{F}(M \otimes W) \arrow[rr] & & 0
\end{tikzcd}$$
e o isomorfismo é natural em V. Tomando $W = V$ e f o morfismo identidade, temos que o isomorfismo não depende da resolução projetiva escolhida.

- Naturalidade em M: Seja $N \in {}^{C}\mathcal{M}$ e $f\colon M \to N$ um morfismo de C-comódulos à esquerda. Pelo Lema 1.29, os seguintes diagramas comutam:

$$\begin{tikzcd}
M^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "f^{(I)}"'] & M^{(J)} \arrow[r] \arrow[d, "f^{(J)}"] & M \otimes V \arrow[r] \arrow[d, "f\otimes V"] & 0 \\
N^{(I)} \arrow[r, "(a_{J,I})"] & N^{(J)} \arrow[r] & N \otimes V \arrow[r] & 0
\end{tikzcd}$$

$$\begin{tikzcd}
\mathcal{F}(M)^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "\mathcal{F}(f)^{(I)}"'] & \mathcal{F}(M)^{(J)} \arrow[r] \arrow[d, "\mathcal{F}(f)^{(J)}"] & \mathcal{F}(M) \otimes V \arrow[r] \arrow[d, "\mathcal{F}(f)\otimes V"] & 0 \\
\mathcal{F}(N)^{(I)} \arrow[r, "(a_{J,I})"] & \mathcal{F}(N)^{(J)} \arrow[r] & \mathcal{F}(N) \otimes V \arrow[r] & 0
\end{tikzcd}$$

Pelo Lema 1.32, os seguintes diagramas comutam:

$$\begin{tikzcd}
\mathcal{F}(M)^{(I)} \arrow[r, "\mathcal{F}(f)^{(I)}"] \arrow[d, "\phi_I"'] & \mathcal{F}(N)^{(I)} \arrow[d, "\phi_I"] \\
\mathcal{F}\big(M^{(I)}\big) \arrow[r, "\mathcal{F}(f^{(I)})"] & \mathcal{F}\big(N^{(I)}\big)
\end{tikzcd}$$

$$\begin{tikzcd}
\mathcal{F}(M)^{(J)} \arrow[r, "\mathcal{F}(f)^{(J)}"] \arrow[d, "\phi_J"'] & \mathcal{F}(N)^{(J)} \arrow[d, "\phi_J"] \\
\mathcal{F}\big(M^{(J)}\big) \arrow[r, "\mathcal{F}(f^{(J)})"] & \mathcal{F}\big(N^{(J)}\big)
\end{tikzcd}$$

Portanto o seguinte diagrama comuta:

$$\begin{tikzcd}
\mathcal{F}(M)^{(I)} \arrow[rr, "(a_{J,I})"] \arrow[dr, "\mathcal{F}(f)^{(I)}"] \arrow[dd, "\phi_I"'] & & \mathcal{F}(M)^{(J)} \arrow[rr] \arrow[dr, "\mathcal{F}(f)^{(J)}"] \arrow[dd, "\phi_J"] & & \mathcal{F}(M)\otimes V \arrow[rr] \arrow[dr, "\mathcal{F}(f)\otimes V"] \arrow[dd, "\theta_V"] & & 0 & \\
& \mathcal{F}(N)^{(I)} \arrow[rr, "(a_{J,I})"] \arrow[dd, "\phi_I"] & & \mathcal{F}(N)^{(J)} \arrow[rr] \arrow[dd, "\phi_J"] & & \mathcal{F}(N)\otimes V \arrow[rr] \arrow[dd, "\theta_W"] & & 0 \\
\mathcal{F}\big(M^{(I)}\big) \arrow[rr, "\mathcal{F}((a_{J,I}))"] \arrow[dr, "\mathcal{F}(f^{(I)})"'] & & \mathcal{F}\big(M^{(J)}\big) \arrow[rr] \arrow[dr, "\mathcal{F}(f^{(J)})"'] & & \mathcal{F}(M\otimes V) \arrow[rr] \arrow[dr, "\mathcal{F}(f\otimes V)"'] & & 0 & \\
& \mathcal{F}\big(N^{(I)}\big) \arrow[rr, "\mathcal{F}((a_{J,I}))"] & & \mathcal{F}\big(N^{(J)}\big) \arrow[rr] & & \mathcal{F}(N\otimes V) \arrow[rr] & & 0
\end{tikzcd}$$

e o isomorfismo é natural em M.

$\square$

1.4 Produto Cotensorial

Seja C uma coálgebra. Se A é um C-comódulo à direita e B é um C-comódulo à esquerda, temos um $\mathbb{K}$-módulo $A\underset{C}{\square}B \subset A \otimes B$, que chamaremos de produto cotensorial de A e B.

Dizemos que um C-comódulo à direita A é C-coplano se $(A\underset{C}{\square}\_)\colon {}^{C}\mathcal{M} \to \mathcal{M}_{\mathbb{K}}$ é um funtor exato.

Nesta seção apresentaremos os conceitos necessários para a demonstração do seguinte resultado: $\mathcal{F}\colon {}^{C}\mathcal{M} \to \mathcal{M}_{\mathbb{K}}$ um funtor exato aditivo que comuta com somas diretas arbitrárias. Então existe um isomorfismo $\mathcal{F}(M) \cong A\underset{C}{\square}M$, natural em $M \in {}^{C}\mathcal{M}$, para algum C-comódulo à direita A que é C-coplano.

Definição 1.34. *Sejam $V, W \in \mathcal{M}_{\mathbb{K}}$ e $f, g\colon V \to W$ morfismos $\mathbb{K}$-lineares. Definimos o equalizador de f e g como sendo o conjunto $\{v \in V;\ f(v) = g(v)\} = \ker(f-g)$.*

Observação 1.35. *Note que, se $h\colon Z \to V$ é um morfismo $\mathbb{K}$-linear tal que $f \circ h = g \circ h$, então $h(Z)$ está contido no equalizador de f e g.*

Denotaremos a categoria dos C-comódulos à direita por $\mathcal{M}^C$.

Definição 1.36. *Seja C uma coálgebra. Para cada $(A, \rho_A) \in \mathcal{M}^C$ e cada $(B, \beta_B) \in {}^C\mathcal{M}$, definimos o produto cotensorial entre A e B, denotado por $A \underset{C}{\square} B$, como o equalizador dos morfismos $(\rho_A \otimes B)$ e $(A \otimes \beta_B)$ e representamos com o seguinte diagrama:*

$$A \underset{C}{\square} B \hookrightarrow A \otimes B \rightrightarrows A \otimes C \otimes B$$

Proposição 1.37. *Sejam C uma coálgebra, (A, ρ) um C-comódulo à direita e (B, β) um C-comódulo à esquerda. Então temos que $A \cong A \underset{C}{\square} C$ e $B \cong C \underset{C}{\square} B$.*

Demonstração. Como A é C-comódulo, temos que:

$$(\rho \otimes C) \circ \rho = (A \otimes \Delta_C) \circ \rho$$

Logo, $\rho(A) \subseteq A \underset{C}{\square} C \subseteq A \otimes C$. Tome $f\colon A \to A \underset{C}{\square} C$ dado por $f(a) = \rho(a)$ e $g\colon A \underset{C}{\square} C \to A$ dado por $g(\sum x_i \otimes c_i) = \sum \varepsilon(c_i) x_i$.

Temos que:

$$\begin{aligned} g \circ f(a) &= g\Big(\sum a_{(0)} \otimes a_{(1)}\Big) \\ &= \sum \varepsilon(a_{(1)}) a_{(0)} \\ &= a \end{aligned}$$

Como $\sum \rho(x_i) \otimes c_i = \sum x_i \otimes \Delta_C(c_i)$, aplicando $(A \otimes C \otimes \varepsilon)$ temos $\sum \varepsilon(c_i)\rho(x_i) = \sum x_i \otimes c_i$. Assim:

$$\begin{aligned} f \circ g(\sum x_i \otimes c_i) &= f\Big(\sum \varepsilon(c_i) x_i\Big) \\ &= \sum \varepsilon(c_i)\rho(x_i) \\ &= \sum x_i \otimes c_i \end{aligned}$$

Portanto, temos que $f \circ g = A \underset{C}{\square} C$ e $g \circ f = A$, o que implica que $A \cong A \underset{C}{\square} C$. De modo análogo, temos que $B \cong C \underset{C}{\square} B$. $\square$

Lema 1.38. *Considere o seguinte diagrama comutativo com a primeira linha exata em $\mathcal{M}_{\mathbb{K}}$:*

$$\begin{tikzcd} 0 \arrow[r] & U \arrow[r, "u"] \arrow[d, "f"'] & V \arrow[r, "v"] \arrow[d, "g"] & W \arrow[d, "h"] \\ 0 \arrow[r] & U' \arrow[r, "u'"] & V' \arrow[r, "v'"] & W' \end{tikzcd}$$

Então temos a seguinte sequência exata:

$$0 \longrightarrow \ker f \xrightarrow{\alpha} \ker g \xrightarrow{\beta} \ker h$$

onde α e β são os morfismos induzidos por u e v respectivamente.

Demonstração. Denotando por i, j e k as inclusões dos núcleos de f, g e h respectivamente, temos o seguinte diagrama comutativo com a segunda linha exata:

$$\begin{tikzcd} & \ker f \arrow[d, "i"'] & \ker g \arrow[d, "j"] & \ker h \arrow[d, "k"] \\ 0 \arrow[r] & U \arrow[r, "u"] \arrow[d, "f"'] & V \arrow[r, "v"] \arrow[d, "g"] & W \arrow[d, "h"] \\ 0 \arrow[r] & U' \arrow[r, "u'"] & V' \arrow[r, "v'"] & W' \end{tikzcd}$$

Note que:

$$g \circ (u \circ i) = u' \circ f \circ i = 0$$
$$h \circ (v \circ j) = v' \circ g \circ j = 0$$

Logo, pela definição de núcleo, existem únicos morfismos:

$$\alpha\colon \ker f \longrightarrow \ker g$$
$$\beta\colon \ker g \longrightarrow \ker h$$

tais que os seguintes diagramas comutam:

$$\begin{tikzcd} \ker f \arrow[r, "\alpha"] \arrow[d, "i"'] & \ker g \arrow[d, "j"] \\ U \arrow[r, "u"] & V \end{tikzcd} \qquad \begin{tikzcd} \ker g \arrow[r, "\beta"] \arrow[d, "j"'] & \ker h \arrow[d, "k"] \\ V \arrow[r, "v"] & W \end{tikzcd}$$

Como k é monomorfismo e:

$$\begin{aligned} k \circ \beta \circ \alpha &= v \circ j \circ \alpha \\ &= v \circ u \circ i \\ &= 0 \end{aligned}$$

temos que $\beta \circ \alpha = 0$.

Seja $y \in \ker \beta$. Como:

$$v \circ j(y) = k \circ \beta(y) = 0$$

temos que $j(y) \in \ker v$. Logo, existe $x \in U$ tal que $u(x) = j(y)$. Assim, temos:

$$\begin{aligned} u' \circ f(x) &= g \circ u(x) \\ &= g \circ j(y) \\ &= 0 \end{aligned}$$

Como u' é monomorfismo, temos que $f(x) = 0$, ou seja, $x \in \ker(f)$. Mas j é monomorfismo e:

$$\begin{aligned} j \circ \alpha(x) &= u \circ i(x) \\ &= u(x) \\ &= j(y) \end{aligned}$$

o que implica que $\alpha(x) = y$, ou seja, a imagem de α é igual ao núcleo de β.

Se $\alpha \circ \Psi = 0$, então:

$$\begin{aligned} 0 &= j \circ \alpha \circ \Psi \\ &= u \circ i \circ \Psi \end{aligned}$$

Como u e i são monomorfismos, temos que $\Psi = 0$. Portanto α é monomorfismo e a seguinte sequência é exata:

$$0 \longrightarrow \ker f \xrightarrow{\alpha} \ker g \xrightarrow{\beta} \ker h$$

$\square$

Proposição 1.39. *Seja C uma coálgebra e A um C-comódulo à direita. Então a aplicação:*

$$\begin{aligned} (A \underset{C}{\square} \_)\colon {}^{C}\mathcal{M} &\longrightarrow \mathcal{M}_{\mathbb{K}} \\ V &\longmapsto A \underset{C}{\square} V \end{aligned}$$

é um funtor exato à esquerda que comuta com somas diretas arbitrárias.

Demonstração. Primeiramente vejamos que $(A\underset{C}{\square}\_)$ é um funtor.

Seja $f\colon V \to W$ um morfismo de C-comódulos. Se $x \otimes v \in A\underset{C}{\square}V$, temos que:

$$\begin{aligned}
(\rho_A \otimes W) \circ (A \otimes f)(x \otimes v) &= (\rho_A \otimes f)(x \otimes v) \\
&= (A \otimes C \otimes f) \circ (\rho_A \otimes V)(x \otimes v) \\
&= (A \otimes C \otimes f) \circ (A \otimes \beta_V)(x \otimes v) \\
&= (A \otimes \beta_W) \circ (A \otimes f)(x \otimes v)
\end{aligned}$$

Pela definição de equalizador, $(A \otimes f)(A\underset{C}{\square}V) \subset A\underset{C}{\square}W$. Logo o seguinte diagrama comuta:

$$\begin{tikzcd}
A\underset{C}{\square}V \arrow[r, hook] \arrow[d, "A\otimes f"'] & A \otimes V \arrow[r, shift left] \arrow[r, shift right] \arrow[d, "A\otimes f"] & A \otimes C \otimes V \arrow[d, "A\otimes C\otimes f"] \\
A\underset{C}{\square}W \arrow[r, hook] & A \otimes W \arrow[r, shift left] \arrow[r, shift right] & A \otimes C \otimes W
\end{tikzcd}$$

Denotaremos por $A\underset{C}{\square}f$ o morfismo $(A \otimes f)|_{A\underset{C}{\square}V}$.

Sejam $f\colon V \to W$ e $g\colon W \to Z$ morfismos de C-comódulos. Temos os seguintes diagramas comutativos:

$$\begin{tikzcd}
A\underset{C}{\square}V \arrow[r, hook] \arrow[d, dotted, "A\underset{C}{\square}f"'] & A \otimes V \arrow[r, shift left] \arrow[r, shift right] \arrow[d, "A\otimes f"] & A \otimes C \otimes V \arrow[d, "A\otimes C\otimes f"] \\
A\underset{C}{\square}W \arrow[r, hook] \arrow[d, dotted, "A\underset{C}{\square}g"'] & A \otimes W \arrow[r, shift left] \arrow[r, shift right] \arrow[d, "A\otimes g"] & A \otimes C \otimes W \arrow[d, "A\otimes C\otimes g"] \\
A\underset{C}{\square}Z \arrow[r, hook] & A \otimes Z \arrow[r, shift left] \arrow[r, shift right] & A \otimes C \otimes Z
\end{tikzcd}$$

e

$$\begin{tikzcd}
A\underset{C}{\square}V \arrow[r, hook] \arrow[d, dotted, "A\underset{C}{\square}gf"'] & A \otimes V \arrow[r, shift left] \arrow[r, shift right] \arrow[d, "A\otimes gf"] & A \otimes C \otimes V \arrow[d, "A\otimes C\otimes gf"] \\
A\underset{C}{\square}Z \arrow[r, hook] & A \otimes Z \arrow[r, shift left] \arrow[r, shift right] & A \otimes C \otimes Z
\end{tikzcd}$$

Como $A \otimes gf = (A \otimes f) \circ (A \otimes g)$, temos que $A\underset{C}{\square}gf = (A\underset{C}{\square}g)(A\underset{C}{\square}f)$ e portanto $(A\underset{C}{\square}\_)$ é um funtor entre as categorias ${}^{C}\mathcal{M}$ e $\mathcal{M}_{\mathbb{K}}$.

Considere a seguinte sequência exata em ${}^{C}\mathcal{M}$:

$$0 \longrightarrow V \xrightarrow{f} W \xrightarrow{g} Z$$

Então temos o seguinte diagrama comutativo com linhas exatas:

$$\begin{tikzcd}
0 \arrow[r] & A \otimes V \arrow[r, "A\otimes f"] \arrow[d, shift left] \arrow[d, shift right] & A \otimes W \arrow[r, "A\otimes g"] \arrow[d, shift left] \arrow[d, shift right] & A \otimes Z \arrow[d, shift left] \arrow[d, shift right] \\
0 \arrow[r] & A \otimes C \otimes V \arrow[r, "A\otimes C\otimes f"] & A \otimes C \otimes W \arrow[r, "A\otimes C\otimes g"] & A \otimes C \otimes Z
\end{tikzcd}$$

Como $A\underset{C}{\square}U = \ker(\rho_A \otimes U - A \otimes \beta_U)$, $\forall U \in {}^{C}\mathcal{M}$, pelo Lema 1.38, temos a seguinte sequência exata:

$$0 \longrightarrow A\underset{C}{\square}V \xrightarrow{A\underset{C}{\square}f} A\underset{C}{\square}W \xrightarrow{A\underset{C}{\square}g} A\underset{C}{\square}Z$$

Portanto o funtor $(A\underset{C}{\square}\_)$ é exato à esquerda.

Seja $(V_i)_{i\in I}$ uma coleção em ${}^{C}\mathcal{M}$. Vejamos que $\bigoplus_{i\in I}(A\underset{C}{\square}V_i) \cong A\underset{C}{\square}(\bigoplus_{i\in I} V_i)$. Para isto, basta mostrar que os seguintes diagramas comutam:

$$\begin{array}{ccc}
\bigoplus_{i\in I}(A\otimes V_i) & \xrightarrow{\bigoplus_{i\in I}(\rho_A\otimes V_i)} & \bigoplus_{i\in I}(A\otimes C\otimes V_i) \\
\cong\downarrow & & \downarrow\cong \\
A\otimes(\bigoplus_{i\in I}V_i) & \xrightarrow{\rho_A\otimes(\bigoplus_{i\in I}V_i)} & A\otimes C\otimes(\bigoplus_{i\in I}V_i)
\end{array}
\qquad
\begin{array}{ccc}
\bigoplus_{i\in I}(A\otimes V_i) & \xrightarrow{\bigoplus_{i\in I}(A\otimes\beta_{V_i})} & \bigoplus_{i\in I}(A\otimes C\otimes V_i) \\
\cong\downarrow & & \downarrow\cong \\
A\otimes(\bigoplus_{i\in I}V_i) & \xrightarrow{A\otimes\beta_{\bigoplus_{i\in I}V_i}} & A\otimes C\otimes(\bigoplus_{i\in I}V_i)
\end{array}$$

De fato:

$$\begin{aligned}
\bigoplus_{i\in I}(\rho_A\otimes V_i)((a\otimes v)_i) &= \bigoplus_{i\in I}\big(\sum a_{(0)}\otimes a_{(1)}\otimes v\big)_i \\
&= \sum a_{(0)}\otimes a_{(1)}\otimes(\bigoplus_{i\in I}(v)_i) \\
&= (\rho_A\otimes(\bigoplus_{i\in I}V_i))(a\otimes(\bigoplus_{i\in I}(v)_i))
\end{aligned}$$

e

$$\begin{aligned}
\bigoplus_{i\in I}(A\otimes\beta_{V_i})((a\otimes v)_i) &= \bigoplus_{i\in I}(a\otimes 1\otimes v)_i \\
&= a\otimes 1\otimes(\bigoplus_{i\in I}(v)_i) \\
&= (A\otimes\beta_{\bigoplus_{i\in I}V_i})(a\otimes(\bigoplus_{i\in I}(v)_i))
\end{aligned}$$

Portanto, existe um isomorfismo que faz o seguinte diagrama comutar:

$$\begin{array}{ccccc}
\bigoplus_{i\in I}(A\underset{C}{\square}V_i) & \hookrightarrow & \bigoplus_{i\in I}(A\otimes V_i) & \rightrightarrows & \bigoplus_{i\in I}(A\otimes C\otimes V_i) \\
\vdots & & \cong\downarrow & & \downarrow\cong \\
A\underset{C}{\square}(\bigoplus_{i\in I}V_i) & \hookrightarrow & A\otimes(\bigoplus_{i\in I}V_i) & \rightrightarrows & A\otimes C\otimes(\bigoplus_{i\in I}V_i)
\end{array}$$

e o funtor $(A\underset{C}{\square}\_)$ comuta com somas diretas. $\square$

Definição 1.40. *Seja M um C-comódulo à direita. Dizemos que M é C-coplano se o funtor $(M\underset{C}{\square}\_)\colon {}^C\mathcal{M}\to\mathcal{M}_{\mathbb{K}}$ é exato.*

Lema 1.41. *Se $M\in\mathcal{M}^C$ é C-coplano, então para qualquer $X\in\mathcal{M}_{\mathbb{K}}$ e $W\in{}^C\mathcal{M}$ a função canônica $(M\underset{C}{\square}W)\otimes X\to M\underset{C}{\square}(W\otimes X)$ é um isomorfismo. Além disso, este isomorfismo é natural em X.*

Em particular, se D é outra coálgebra $\mathbb{K}$-plana, $W\in{}^C\mathcal{M}^D$ e $U\in{}^D\mathcal{M}$, então o produto cotensorial é associativo:

$$(M\underset{C}{\square}W)\underset{D}{\square}U\cong M\underset{C}{\square}(W\underset{D}{\square}U)$$

Demonstração. Seja $W\in{}^C\mathcal{M}$. Para cada conjunto I de índices, considere os seguintes isomorfismos:

$$\begin{aligned}
M\otimes\big(W\otimes\mathbb{K}^{(I)}\big) &\xrightarrow{\cong}(M\otimes W)\otimes\mathbb{K}^{(I)} \\
m\otimes(w\otimes(\lambda)_i) &\longmapsto(m\otimes w)\otimes(\lambda)_i
\end{aligned}$$

$$\begin{aligned}
M\otimes C\otimes\big(W\otimes\mathbb{K}^{(I)}\big) &\xrightarrow{\cong}(M\otimes C\otimes W)\otimes\mathbb{K}^{(I)} \\
m\otimes c\otimes(w\otimes(\lambda)_i) &\longmapsto(m\otimes c\otimes w)\otimes(\lambda)_i
\end{aligned}$$

Claramente os seguintes diagramas comutam com os isomorfismos acima:

$$\begin{tikzcd}
M \otimes \left(W \otimes \mathbb{K}^{(I)}\right) \arrow[r, "\rho_M \otimes (W \otimes \mathbb{K}^{(I)})"] \arrow[d, "\cong"'] & M \otimes C \otimes \left(W \otimes \mathbb{K}^{(I)}\right) \arrow[d, "\cong"] \\
(M \otimes W) \otimes \mathbb{K}^{(I)} \arrow[r, "(\rho_M \otimes W) \otimes \mathbb{K}^{(I)}"] & (M \otimes C \otimes W) \otimes \mathbb{K}^{(I)}
\end{tikzcd}$$

$$\begin{tikzcd}
M \otimes \left(W \otimes \mathbb{K}^{(I)}\right) \arrow[r, "M \otimes (\beta_W \otimes \mathbb{K}^{(I)})"] \arrow[d, "\cong"'] & M \otimes C \otimes \left(W \otimes \mathbb{K}^{(I)}\right) \arrow[d, "\cong"] \\
(M \otimes W) \otimes \mathbb{K}^{(I)} \arrow[r, "(M \otimes \beta_W) \otimes \mathbb{K}^{(I)}"] & (M \otimes C \otimes W) \otimes \mathbb{K}^{(I)}
\end{tikzcd}$$

Logo, temos um isomorfismo entre $M \underset{C}{\square} \left(W \otimes \mathbb{K}^{(I)}\right)$ e $(M \underset{C}{\square} W) \otimes \mathbb{K}^{(I)}$ que faz o seguinte diagrama comutar:

$$\begin{tikzcd}
M \underset{C}{\square} \left(W \otimes \mathbb{K}^{(I)}\right) \arrow[r, hook] \arrow[d, dotted] & M \otimes \left(W \otimes \mathbb{K}^{(I)}\right) \arrow[r, shift left] \arrow[r, shift right] \arrow[d, "\cong"] & M \otimes C \otimes \left(W \otimes \mathbb{K}^{(I)}\right) \arrow[d, "\cong"] \\
(M \underset{C}{\square} W) \otimes \mathbb{K}^{(I)} \arrow[r, hook] & (M \otimes W) \otimes \mathbb{K}^{(I)} \arrow[r, shift left] \arrow[r, shift right] & (M \otimes C \otimes W) \otimes \mathbb{K}^{(I)}
\end{tikzcd}$$

Tome $X \in \mathcal{M}_{\mathbb{K}}$ e considere uma resolução projetiva de X:

$$\mathbb{K}^{(I)} \xrightarrow{(a_{J,I})} \mathbb{K}^{(J)} \longrightarrow X \longrightarrow 0$$

Nos diagramas a seguir, os morfismos são os induzidos pelos funtores aplicados e os isomorfismos são os da construção acima. Apenas explicitaremos o morfismo no diagrama quando o mesmo não estiver claro pelo contexto.

Como os funtores $(W \otimes \_)$, $(M \underset{C}{\square} \_)$ e $((M \underset{C}{\square} W) \otimes \_)$ são exatos, temos as seguintes sequências exatas:

$$M \underset{C}{\square} (W \otimes \mathbb{K}^{(I)}) \longrightarrow M \underset{C}{\square} (W \otimes \mathbb{K}^{(J)}) \longrightarrow M \underset{C}{\square} (W \otimes X) \longrightarrow 0$$

e

$$(M \underset{C}{\square} W) \otimes \mathbb{K}^{(I)} \longrightarrow (M \underset{C}{\square} W) \otimes \mathbb{K}^{(J)} \longrightarrow (M \underset{C}{\square} W) \otimes X \longrightarrow 0$$

Sejam Φ e Ψ os morfismos determinados pelos seguintes diagramas comutativos:

$$\begin{tikzcd}
M \otimes (W \otimes \mathbb{K}^{(I)}) \arrow[r] \arrow[d, "\cong"'] \arrow[dr, dotted, "\Phi"] & M \otimes (W \otimes \mathbb{K}^{(J)}) \arrow[d, "\cong"] \\
(M \otimes W) \otimes \mathbb{K}^{(I)} \arrow[r] & (M \otimes W) \otimes \mathbb{K}^{(J)}
\end{tikzcd}$$

$$\begin{tikzcd}
M \otimes C \otimes (W \otimes \mathbb{K}^{(I)}) \arrow[r] \arrow[d, "\cong"'] \arrow[dr, dotted, "\Psi"] & M \otimes C \otimes (W \otimes \mathbb{K}^{(J)}) \arrow[d, "\cong"] \\
(M \otimes C \otimes W) \otimes \mathbb{K}^{(I)} \arrow[r] & (M \otimes C \otimes W) \otimes \mathbb{K}^{(J)}
\end{tikzcd}$$

Como os seguintes diagramas comutam:

$$\begin{tikzcd}
M \otimes (W \otimes \mathbb{K}^{(I)}) \arrow[r, "\rho_M \otimes (W \otimes \mathbb{K}^{(I)})"] \arrow[d] & M \otimes C \otimes (W \otimes \mathbb{K}^{(I)}) \arrow[d] \\
M \otimes (W \otimes \mathbb{K}^{(J)}) \arrow[r, "\rho_M \otimes (W \otimes \mathbb{K}^{(J)})"] \arrow[d, "\cong"'] & M \otimes C \otimes (W \otimes \mathbb{K}^{(J)}) \arrow[d, "\cong"] \\
(M \otimes W) \otimes \mathbb{K}^{(J)} \arrow[r, "(\rho_M \otimes W) \otimes \mathbb{K}^{(J)}"] & (M \otimes C \otimes W) \otimes \mathbb{K}^{(J)}
\end{tikzcd}$$

$$\begin{tikzcd}
M \otimes (W \otimes \mathbb{K}^{(I)}) \arrow[r, "M\otimes(\beta_W \otimes \mathbb{K}^{(I)})"] \arrow[d, "\cong"'] & M \otimes C \otimes (W \otimes \mathbb{K}^{(I)}) \arrow[d, "\cong"] \\
(M \otimes W) \otimes \mathbb{K}^{(I)} \arrow[r, "(M\otimes\beta_W)\otimes\mathbb{K}^{(I)}"] \arrow[d] & (M \otimes C \otimes W) \otimes \mathbb{K}^{(I)} \arrow[d] \\
(M \otimes W) \otimes \mathbb{K}^{(J)} \arrow[r, "(M\otimes\beta_W)\otimes\mathbb{K}^{(J)}"] & (M \otimes C \otimes W) \otimes \mathbb{K}^{(J)}
\end{tikzcd}$$

temos que o seguinte diagrama comuta:

$$\begin{tikzcd}
M \otimes \big(W \otimes \mathbb{K}^{(I)}\big) \arrow[r, shift left] \arrow[r, shift right] \arrow[d, "\Phi"'] & M \otimes C \otimes \big(W \otimes \mathbb{K}^{(I)}\big) \arrow[d, "\Psi"] \\
(M \otimes W) \otimes \mathbb{K}^{(J)} \arrow[r, shift left] \arrow[r, shift right] & (M \otimes C \otimes W) \otimes \mathbb{K}^{(J)}
\end{tikzcd}$$

As compostas:

$$M\underset{C}{\square}(W \otimes \mathbb{K}^{(I)}) \longrightarrow M\underset{C}{\square}(W \otimes \mathbb{K}^{(J)}) \xrightarrow{\cong} (M\underset{C}{\square}W) \otimes \mathbb{K}^{(J)}$$

$$M\underset{C}{\square}(W \otimes \mathbb{K}^{(I)}) \xrightarrow{\cong} (M\underset{C}{\square}W) \otimes \mathbb{K}^{(I)} \longrightarrow (M\underset{C}{\square}W) \otimes \mathbb{K}^{(J)}$$

satisfazem o seguinte diagrama comutativo:

$$\begin{tikzcd}
M\underset{C}{\square}\big(W \otimes \mathbb{K}^{(I)}\big) \arrow[r, hook] \arrow[d, dotted] & M \otimes \big(W \otimes \mathbb{K}^{(I)}\big) \arrow[r, shift left] \arrow[r, shift right] \arrow[d, "\Phi"] & M \otimes C \otimes \big(W \otimes \mathbb{K}^{(I)}\big) \arrow[d, "\Psi"] \\
(M\underset{C}{\square}W) \otimes \mathbb{K}^{(J)} \arrow[r, hook] & (M \otimes W) \otimes \mathbb{K}^{(J)} \arrow[r, shift left] \arrow[r, shift right] & (M \otimes C \otimes W) \otimes \mathbb{K}^{(J)}
\end{tikzcd}$$

Pela unicidade do morfismo que satisfaz o diagrama acima, temos que o seguinte diagrama comuta:

$$\begin{tikzcd}
M\underset{C}{\square}(W \otimes \mathbb{K}^{(I)}) \arrow[r] \arrow[d, "\cong"'] & M\underset{C}{\square}(W \otimes \mathbb{K}^{(J)}) \arrow[d, "\cong"] \\
(M\underset{C}{\square}W) \otimes \mathbb{K}^{(I)} \arrow[r] & (M\underset{C}{\square}W) \otimes \mathbb{K}^{(J)}
\end{tikzcd}$$

e existe um único isomorfismo $f_X \colon M\underset{C}{\square}(W \otimes X) \to (M\underset{C}{\square}W) \otimes X$ que faz o seguinte diagrama comutar:

$$\begin{tikzcd}
M\underset{C}{\square}(W \otimes \mathbb{K}^{(I)}) \arrow[r] \arrow[d, "\cong"'] & M\underset{C}{\square}(W \otimes \mathbb{K}^{(J)}) \arrow[r] \arrow[d, "\cong"] & M\underset{C}{\square}(W \otimes X) \arrow[r] \arrow[d, dotted, "f_X"] & 0 \\
(M\underset{C}{\square}W) \otimes \mathbb{K}^{(I)} \arrow[r] & (M\underset{C}{\square}W) \otimes \mathbb{K}^{(J)} \arrow[r] & (M\underset{C}{\square}W) \otimes X \arrow[r] & 0
\end{tikzcd}$$

Naturalidade em X: A naturalidade em X é provada juntamente com a independência da escolha da resolução projetiva. Seja $Y \in \mathcal{M}_{\mathbb{K}}$ um outro $\mathbb{K}$-módulo. Tome uma resolução projetiva de Y:

$$\mathbb{K}^{(K)} \xrightarrow{(b_{L,K})} \mathbb{K}^{(L)} \longrightarrow Y \longrightarrow 0$$

e $g \colon X \to Y$ um morfismo de $\mathbb{K}$-módulos. Pelo teorema da comparação para resoluções projetivas, existem morfismos $(c_{K,I}) \colon \mathbb{K}^{(I)} \to \mathbb{K}^{(K)}$ e $(d_{L,J}) \colon \mathbb{K}^{(J)} \to \mathbb{K}^{(L)}$ que fazem o seguinte diagrama comutar:

$$\begin{tikzcd}
\mathbb{K}^{(I)} \arrow[r, "(a_{J,I})"] \arrow[d, "(c_{K,I})"'] & \mathbb{K}^{(J)} \arrow[r] \arrow[d, "(d_{L,J})"] & X \arrow[r] \arrow[d, "g"] & 0 \\
\mathbb{K}^{(K)} \arrow[r, "(b_{L,K})"] & \mathbb{K}^{(L)} \arrow[r] & Y \arrow[r] & 0
\end{tikzcd}$$

Aplicando os funtores $(M\underset{C}{\square}(W\otimes \_))$ e $((M\underset{C}{\square}W)\otimes \_)$ no diagrama acima, temos os seguintes diagramas comutativos:

$$\begin{tikzcd}
M\underset{C}{\square}(W\otimes \mathbb{K}^{(I)}) \arrow[r] \arrow[d] & M\underset{C}{\square}(W\otimes \mathbb{K}^{(J)}) \arrow[r] \arrow[d] & M\underset{C}{\square}(W\otimes X) \arrow[r] \arrow[d] & 0 \\
M\underset{C}{\square}(W\otimes \mathbb{K}^{(K)}) \arrow[r] & M\underset{C}{\square}(W\otimes \mathbb{K}^{(L)}) \arrow[r] & M\underset{C}{\square}(W\otimes Y) \arrow[r] & 0
\end{tikzcd}$$

$$\begin{tikzcd}
(M\underset{C}{\square}W)\otimes \mathbb{K}^{(I)} \arrow[r] \arrow[d] & (M\underset{C}{\square}W)\otimes \mathbb{K}^{(J)} \arrow[r] \arrow[d] & (M\underset{C}{\square}W)\otimes X \arrow[r] \arrow[d] & 0 \\
(M\underset{C}{\square}W)\otimes \mathbb{K}^{(K)} \arrow[r] & (M\underset{C}{\square}W)\otimes \mathbb{K}^{(L)} \arrow[r] & (M\underset{C}{\square}W)\otimes Y \arrow[r] & 0
\end{tikzcd}$$

Além disso, do mesmo modo que provamos a comutatividade do diagrama:

$$\begin{tikzcd}
M\underset{C}{\square}(W\otimes \mathbb{K}^{(I)}) \arrow[r] \arrow[d, "\cong"'] & M\underset{C}{\square}(W\otimes \mathbb{K}^{(J)}) \arrow[d, "\cong"] \\
(M\underset{C}{\square}W)\otimes \mathbb{K}^{(I)} \arrow[r] & (M\underset{C}{\square}W)\otimes \mathbb{K}^{(J)}
\end{tikzcd}$$

podemos verificar que os diagramas a seguir comutam:

$$\begin{tikzcd}
M\underset{C}{\square}(W\otimes \mathbb{K}^{(K)}) \arrow[r] \arrow[d, "\cong"'] & M\underset{C}{\square}(W\otimes \mathbb{K}^{(L)}) \arrow[d, "\cong"] \\
(M\underset{C}{\square}W)\otimes \mathbb{K}^{(K)} \arrow[r] & (M\underset{C}{\square}W)\otimes \mathbb{K}^{(L)}
\end{tikzcd}$$

$$\begin{tikzcd}
M\underset{C}{\square}(W\otimes \mathbb{K}^{(I)}) \arrow[r] \arrow[d, "\cong"'] & M\underset{C}{\square}(W\otimes \mathbb{K}^{(K)}) \arrow[d, "\cong"] \\
(M\underset{C}{\square}W)\otimes \mathbb{K}^{(I)} \arrow[r] & (M\underset{C}{\square}W)\otimes \mathbb{K}^{(K)}
\end{tikzcd}$$

$$\begin{tikzcd}
M\underset{C}{\square}(W\otimes \mathbb{K}^{(J)}) \arrow[r] \arrow[d, "\cong"'] & M\underset{C}{\square}(W\otimes \mathbb{K}^{(L)}) \arrow[d, "\cong"] \\
(M\underset{C}{\square}W)\otimes \mathbb{K}^{(J)} \arrow[r] & (M\underset{C}{\square}W)\otimes \mathbb{K}^{(L)}
\end{tikzcd}$$

Portanto o seguinte diagrama comuta:

$$\begin{tikzcd}
M\underset{C}{\square}(W\otimes \mathbb{K}^{(I)}) \arrow[rr] \arrow[dr] \arrow[dd, "\cong"'] & & M\underset{C}{\square}(W\otimes \mathbb{K}^{(J)}) \arrow[rr] \arrow[dr] \arrow[dd, "\cong"] & & M\underset{C}{\square}(W\otimes X) \arrow[rr] \arrow[dr] \arrow[dd, "f_X"] & & 0 \\
& M\underset{C}{\square}(W\otimes \mathbb{K}^{(K)}) \arrow[rr] \arrow[dd, "\cong"'] & & M\underset{C}{\square}(W\otimes \mathbb{K}^{(L)}) \arrow[rr] \arrow[dd, "\cong"'] & & M\underset{C}{\square}(W\otimes Y) \to 0 \arrow[dd, "f_Y"] & \\
(M\underset{C}{\square}W)\otimes \mathbb{K}^{(I)} \arrow[rr] \arrow[dr] & & (M\underset{C}{\square}W)\otimes \mathbb{K}^{(J)} \arrow[rr] \arrow[dr] & & (M\underset{C}{\square}W)\otimes X \arrow[rr] \arrow[dr] & & 0 \\
& (M\underset{C}{\square}W)\otimes \mathbb{K}^{(K)} \arrow[rr] & & (M\underset{C}{\square}W)\otimes \mathbb{K}^{(L)} \arrow[rr] & & (M\underset{C}{\square}W)\otimes Y \to 0 &
\end{tikzcd}$$

e o isomorfismo é natural em X. Tomando $Y = X$ e g o morfismo identidade, temos que o isomorfismo não depende da resolução projetiva escolhida. $\square$

Observação 1.42. *Utilizando um abuso de linguagem, diremos que uma sequência da forma:*

$$0 \longrightarrow V \longrightarrow W \underset{g}{\overset{f}{\rightrightarrows}} Z$$

é exata se a sequência:

$$0 \longrightarrow V \longrightarrow W \xrightarrow{f-g} Z$$

é exata.

Agora apresentaremos o resultado principal desta seção.

Teorema 1.43. *Seja C uma coálgebra, e $\mathcal{F}\colon {}^{C}\mathcal{M} \to \mathcal{M}_{\mathbb{K}}$ um funtor exato aditivo que comuta com somas diretas arbitrárias. Então existe um isomorfismo $\mathcal{F}(M) \cong A \underset{C}{\square} M$, natural em $M \in {}^{C}\mathcal{M}$, para algum comódulo $A \in \mathcal{M}^{C}$ que é C-coplano.*

Demonstração. Seja $\theta\colon \mathcal{F}(C \otimes V) \to \mathcal{F}(C) \otimes V$, $\forall V \in \mathcal{M}_{\mathbb{K}}$ o isomorfismo dado pelo Teorema 1.33.

Tome $A = \mathcal{F}(C)$ e ρ_A a composição:

$$A = \mathcal{F}(C) \xrightarrow{\mathcal{F}(\Delta_C)} \mathcal{F}(C \otimes C) \xrightarrow{\ \ \theta\ \ } \mathcal{F}(C) \otimes C = A \otimes C$$

Então A é um C-comódulo à direita. Vejamos que $\mathcal{F}(M) \cong A \underset{C}{\square} M$, $\forall (M, \beta_M) \in {}^{C}\mathcal{M}$. De fato, pela Proposição 1.37, temos que $M \cong C \underset{C}{\square} M$. Logo, temos que a seguinte sequência é exata:

$$0 \longrightarrow M \longrightarrow C \otimes M \rightrightarrows C \otimes C \otimes M$$

Aplicando o funtor $\mathcal{F}$, temos:

$$0 \longrightarrow \mathcal{F}(M) \longrightarrow \mathcal{F}(C \otimes M) \rightrightarrows \mathcal{F}(C \otimes C \otimes M)$$

Como θ é natural em V, temos que o seguinte diagrama comuta:

$$\begin{tikzcd}
\mathcal{F}(C \otimes M) \arrow[r, "\mathcal{F}(C\otimes\beta_M)"] \arrow[d, "\theta"'] & \mathcal{F}\big(C \otimes (C \otimes M)\big) \arrow[d, "\theta"] \\
\mathcal{F}(C) \otimes M \arrow[r, "\mathcal{F}(C)\otimes\beta_M"] & \mathcal{F}(C) \otimes (C \otimes M)
\end{tikzcd}$$

Como θ é natural em C, temos que o seguinte diagrama comuta:

$$\begin{tikzcd}
\mathcal{F}(C \otimes M) \arrow[r, "\mathcal{F}(\Delta\otimes M)"] \arrow[d, "\theta"'] & \mathcal{F}\big((C \otimes C) \otimes M\big) \arrow[d, "\theta"] \\
\mathcal{F}(C) \otimes M \arrow[r, "\mathcal{F}(\Delta)\otimes M"] & \mathcal{F}(C \otimes C) \otimes M
\end{tikzcd}$$

Além disso, pela definição de ρ_A, o seguinte diagrama comuta:

$$\begin{tikzcd}
\mathcal{F}(C) \otimes M \arrow[r, "\mathcal{F}(\Delta)\otimes M"] \arrow[d, equal] & \mathcal{F}(C \otimes C) \otimes M \arrow[d, "\theta\otimes M"] \\
\mathcal{F}(C) \otimes M \arrow[r, "\rho_A\otimes M"] & \mathcal{F}(C) \otimes C \otimes M
\end{tikzcd}$$

Portanto o seguinte diagrama comuta:

$$\begin{tikzcd}
\mathcal{F}(C \otimes M) \arrow[r, "\mathcal{F}(\Delta\otimes M)"] \arrow[d, "\theta"'] & \mathcal{F}\big((C \otimes C) \otimes M\big) \arrow[d, "\theta"] \\
\mathcal{F}(C) \otimes M \arrow[r, "\mathcal{F}(\Delta)\otimes M"] \arrow[d, equal] & \mathcal{F}(C \otimes C) \otimes M \arrow[d, "\theta\otimes M"] \\
\mathcal{F}(C) \otimes M \arrow[r, "\rho_A\otimes M"] & \mathcal{F}(C) \otimes C \otimes M
\end{tikzcd}$$

Como θ é coerente, os isomorfismos:

$$(\theta \otimes M) \circ \theta \colon \mathcal{F}\big((C \otimes C) \otimes M\big) \longrightarrow \mathcal{F}(C) \otimes C \otimes M$$

e

$$\theta \colon \mathcal{F}\big(C \otimes (C \otimes M)\big) \longrightarrow \mathcal{F}(C) \otimes C \otimes M$$

coincidem.

Logo, existe um isomorfismo $\psi_M \colon \mathcal{F}(M) \to \mathcal{F}(C)\underset{C}{\square}M$ que faz o seguinte diagrama comutar:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{F}(M) \arrow[r] \arrow[d, dotted, "\psi_M"'] & \mathcal{F}(C \otimes M) \arrow[r, shift left] \arrow[r, shift right] \arrow[d, "\theta"] & \mathcal{F}(C \otimes C \otimes M) \arrow[d, "\theta"] \\
0 \arrow[r] & \mathcal{F}(C)\underset{C}{\square}M \arrow[r] & \mathcal{F}(C) \otimes M \arrow[r, shift left] \arrow[r, shift right] & \mathcal{F}(C) \otimes C \otimes M
\end{tikzcd}$$

Portanto $\mathcal{F}(M) \cong A\underset{C}{\square}M$. Como o funtor $\mathcal{F}$ é exato, A é C-coplano.

Vejamos a naturalidade em M: Seja (N, β_N) outro C-comódulo à esquerda e $f \colon M \to N$ um morfismo de C-comódulos à esquerda.

Como f é morfismo de C-comódulos à esquerda, os seguintes diagramas comutam:

$$\begin{tikzcd}
M \arrow[r, "\beta_M"] \arrow[d, "f"'] & C \otimes M \arrow[d, "C\otimes f"] \\
N \arrow[r, "\beta_N"] & C \otimes N
\end{tikzcd}
\qquad
\begin{tikzcd}
C \otimes M \arrow[r, "C\otimes\beta_M"] \arrow[d, "C\otimes f"'] & C \otimes C \otimes M \arrow[d, "C\otimes C\otimes f"] \\
C \otimes N \arrow[r, "C\otimes\beta_N"] & C \otimes C \otimes N
\end{tikzcd}$$

Claramente o seguinte diagrama comuta:

$$\begin{tikzcd}
C \otimes M \arrow[r, "\Delta\otimes M"] \arrow[d, "C\otimes f"'] & C \otimes C \otimes M \arrow[d, "C\otimes C\otimes f"] \\
C \otimes N \arrow[r, "\Delta\otimes N"] & C \otimes C \otimes N
\end{tikzcd}$$

Logo o seguinte diagrama comuta:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\beta_M"] \arrow[d, "f"'] & C \otimes M \arrow[r, shift left] \arrow[r, shift right] \arrow[d, "C\otimes f"] & C \otimes C \otimes M \arrow[d, "C\otimes C\otimes f"] \\
0 \arrow[r] & N \arrow[r, "\beta_N"] & C \otimes N \arrow[r, shift left] \arrow[r, shift right] & C \otimes C \otimes N
\end{tikzcd}$$

Durante a demonstração da Proposição 1.39, verificamos que o seguinte diagrama comuta:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{F}(C)\underset{C}{\square}M \arrow[r] \arrow[d, "\mathcal{F}(C)\underset{C}{\square}f"'] & \mathcal{F}(C) \otimes M \arrow[r, shift left] \arrow[r, shift right] \arrow[d, "\mathcal{F}(C)\otimes f"] & \mathcal{F}(C) \otimes C \otimes M \arrow[d, "\mathcal{F}(C)\otimes C\otimes f"] \\
0 \arrow[r] & \mathcal{F}(C)\underset{C}{\square}N \arrow[r] & \mathcal{F}(C) \otimes N \arrow[r, shift left] \arrow[r, shift right] & \mathcal{F}(C) \otimes C \otimes N
\end{tikzcd}$$

Além disso, como θ é natural em V, os seguintes diagramas comutam:

$$\begin{tikzcd}
\mathcal{F}(C \otimes M) \arrow[r, "\mathcal{F}(C\otimes f)"] \arrow[d, "\theta"'] & \mathcal{F}(C \otimes N) \arrow[d, "\theta"] \\
\mathcal{F}(C) \otimes M \arrow[r, "\mathcal{F}(C)\otimes f"] & \mathcal{F}(C) \otimes N
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathcal{F}(C \otimes C \otimes M) \arrow[r, "\mathcal{F}(C\otimes C\otimes f)"] \arrow[d, "\theta"'] & \mathcal{F}(C \otimes C \otimes N) \arrow[d, "\theta"] \\
\mathcal{F}(C) \otimes C \otimes M \arrow[r, "\mathcal{F}(C)\otimes C\otimes f"] & \mathcal{F}(C) \otimes C \otimes N
\end{tikzcd}$$

Portanto o seguinte diagrama comuta:

$$
\begin{tikzcd}[column sep=small]
0 \arrow[r] & \mathcal{F}(M) \arrow[rr] \arrow[dr, "\mathcal{F}(f)"] \arrow[dd, "\psi_M"'] & & \mathcal{F}(C\otimes M) \arrow[rr, shift left] \arrow[rr, shift right] \arrow[dr, "\mathcal{F}(C\otimes f)"] \arrow[dd, "\theta"] & & \mathcal{F}(C\otimes C\otimes M) \arrow[dr, "\mathcal{F}(C\otimes C\otimes f)"] \arrow[dd, "\theta"] & \\
& 0 \arrow[r] & \mathcal{F}(N) \arrow[rr] \arrow[dd, "\psi_N"] & & \mathcal{F}(C\otimes N) \arrow[rr, shift left] \arrow[rr, shift right] \arrow[dd, "\theta"] & & \mathcal{F}(C\otimes C\otimes N) \arrow[dd, "\theta"] \\
0 \arrow[r] & \mathcal{F}(C)\underset{C}{\square}M \arrow[rr] \arrow[dr, "\mathcal{F}(C)\underset{C}{\square}f"'] & & \mathcal{F}(C)\otimes M \arrow[rr, shift left] \arrow[rr, shift right] \arrow[dr, "\mathcal{F}(C)\otimes f"'] & & \mathcal{F}(C)\otimes C\otimes M \arrow[dr, "\mathcal{F}(C)\otimes C\otimes f"'] & \\
& 0 \arrow[r] & \mathcal{F}(C)\underset{C}{\square}N \arrow[rr] & & \mathcal{F}(C)\otimes N \arrow[rr, shift left] \arrow[rr, shift right] & & \mathcal{F}(C)\otimes C\otimes N
\end{tikzcd}
$$

e o isomorfismo é natural em M. □

1.5 Biálgebras e Álgebras de Hopf

Nesta seção apresentaremos alguns resultados sobre biálgebras, quociente de biálgebras e introduziremos o conceito de álgebra de Hopf.

Definição 1.44. *Seja B uma coálgebra que também é uma álgebra. Diremos que B é uma biálgebra se Δ_B e ε_B são morfismos de álgebras.*

Definição 1.45. *Sejam A, B biálgebras e $f\colon A \to B$ um morfismo $\mathbb{K}$-linear. Diremos que f é morfismo de biálgebras se f é morfismo de álgebras e de coálgebras.*

Proposição 1.46. *Sejam M uma coálgebra e L a álgebra tensorial sobre M. Então existe uma única estrutura de coálgebra para L tal que L é biálgebra e o morfismo inclusão $\iota\colon M \to L$ é morfismo de coálgebras.*

Demonstração. Pela definição de álgebra tensorial, existem únicos morfismos de álgebras Δ_L e ε_L tais que os seguintes diagramas comutam:

$$
\begin{tikzcd}
& L \arrow[d, dotted, "\Delta_L"] \\
M \arrow[ur, "\iota"] \arrow[r, "(\iota\otimes\iota)\circ\Delta_M"'] & L\otimes L
\end{tikzcd}
\qquad
\begin{tikzcd}
& L \arrow[d, dotted, "\varepsilon_L"] \\
M \arrow[ur, "\iota"] \arrow[r, "\varepsilon_M"'] & \mathbb{K}
\end{tikzcd}
$$

Note que, se L for coálgebra, então pela comutatividade destes dois diagramas, temos que ι é morfismo de coálgebras.

Vejamos que de fato $(L, \Delta_L, \varepsilon_L)$ é coálgebra:

$$
\begin{aligned}
(\Delta_L \otimes L) \circ \Delta_L \circ \iota &= (\Delta_L \otimes L) \circ (\iota \otimes \iota) \circ \Delta_M \\
&= \big((\Delta_L \circ \iota) \otimes \iota\big) \circ \Delta_M \\
&= \Big(\big((\iota \otimes \iota) \circ \Delta_M\big) \otimes \iota\Big) \circ \Delta_M \\
&= (\iota \otimes \iota \otimes \iota) \circ (\Delta_M \otimes M) \circ \Delta_M \\
&= (\iota \otimes \iota \otimes \iota) \circ (M \otimes \Delta_M) \circ \Delta_M \\
&= \big(\iota \otimes ((\iota \otimes \iota) \circ \Delta_M)\big) \circ \Delta_M \\
&= \big(\iota \otimes (\Delta_L \circ \iota)\big) \circ \Delta_M \\
&= (L \otimes \Delta_L) \circ (\iota \otimes \iota) \circ \Delta_M \\
&= (L \otimes \Delta_L) \circ \Delta_L \circ \iota
\end{aligned}
$$

Logo, tomando $f = (\iota \otimes \iota \otimes \iota) \circ (\Delta_M \otimes M) \circ \Delta_M = (\iota \otimes \iota \otimes \iota) \circ (M \otimes \Delta_M) \circ \Delta_M$, temos que $(\Delta_L \otimes L) \circ \Delta_L$ e $(L \otimes \Delta_L) \circ \Delta_L$ fazem o seguinte diagrama comutar:

$$\begin{tikzcd} & & L \arrow[d, dotted] \\ M \arrow[urr, "\iota"] \arrow[rr, "f"'] & & L \otimes L \otimes L \end{tikzcd}$$

Pela definição de álgebra tensorial, temos que $(\Delta_L \otimes L) \circ \Delta_L = (L \otimes \Delta_L) \circ \Delta_L$.

Além disso, temos:

$$\begin{aligned} (L \otimes \varepsilon_L) \circ \Delta_L \circ \iota &= (L \otimes \varepsilon_L) \circ (\iota \otimes \iota) \circ \Delta_M \\ &= \big(\iota \otimes (\varepsilon_L \circ \iota)\big) \circ \Delta_M \\ &= (\iota \otimes \varepsilon_M) \circ \Delta_M \\ &= (\iota \otimes \mathbb{K}) \circ (M \otimes \varepsilon_M) \circ \Delta_M \\ &= (\iota \otimes \mathbb{K}) \circ \tau_M \\ &= \tau_L \circ \iota \end{aligned}$$

Logo, tomando $f = (\iota \otimes \mathbb{K}) \circ \tau_M$, temos que $(L \otimes \varepsilon_L) \circ \Delta_L$ e τ_L fazem o seguinte diagrama comutar:

$$\begin{tikzcd} & & L \arrow[d, dotted] \\ M \arrow[urr, "\iota"] \arrow[rr, "f"'] & & L \otimes \mathbb{K} \end{tikzcd}$$

Pela definição de álgebra tensorial, temos que $(L \otimes \varepsilon_L) \circ \Delta_L = \tau_L$. À esquerda temos um resultado análogo.

Portanto $(L, \Delta_L, \varepsilon_L)$ é coálgebra e ι é morfismo de coálgebras. Além disso, como Δ_L e ε_L são morfismos de álgebras, temos que L é biálgebra. □

Definição 1.47. *Seja $(C, \Delta_C, \varepsilon_C)$ uma coálgebra e I um $\mathbb{K}$-submódulo de C. Diremos que I é um coideal de C se:*

$$\Delta_C(I) \subset I \otimes C + C \otimes I \quad e \quad \varepsilon_C(I) = 0$$

Proposição 1.48. *Sejam B uma biálgebra e I um ideal de B que também é um coideal de B. Então existe uma única estrutura de biálgebra no quociente B/I para o qual o morfismo projeção $\pi_I \colon B \to B/I$ é morfismo de biálgebras.*

Demonstração. Pela proposição B.7, temos que existem únicos morfismos de álgebras $\Delta_{B/I}$ e $\varepsilon_{B/I}$ que fazem os seguintes diagramas comutarem:

$$\begin{tikzcd} B \arrow[rr, "(\pi_I \otimes \pi_I) \circ \Delta_B"] \arrow[dr, "\pi_I"'] & & B/I \otimes B/I \\ & B/I \arrow[ur, dotted, "\Delta_{B/I}"'] & \end{tikzcd} \qquad \begin{tikzcd} B \arrow[rr, "\varepsilon_B"] \arrow[dr, "\pi_I"'] & & \mathbb{K} \\ & B/I \arrow[ur, dotted, "\varepsilon_{B/I}"'] & \end{tikzcd}$$

Vejamos que $(B/I, \Delta_{B/I}, \varepsilon_{B/I})$ é uma coálgebra. Precisamos que os seguintes diagramas comutem:

$$\begin{tikzcd} B/I \arrow[r, "\Delta_{B/I}"] \arrow[d, "\Delta_{B/I}"'] & B/I \otimes B/I \arrow[d, "B/I \otimes \Delta_{B/I}"] \\ B/I \otimes B/I \arrow[r, "\Delta_{B/I} \otimes B/I"] & B/I \otimes B/I \otimes B/I \end{tikzcd}$$

$$\begin{tikzcd}
 & B/I \arrow[dl, "\cong"'] \arrow[dr, "\cong"] \arrow[dd, "\Delta_{B/I}"] & \\
\mathbb{K} \otimes B/I & & B/I \otimes \mathbb{K} \\
 & B/I \otimes B/I \arrow[ul, "\varepsilon_{B/I} \otimes B/I"] \arrow[ur, "B/I \otimes \varepsilon_{B/I}"'] &
\end{tikzcd}$$

De fato, temos:

$$\begin{aligned}
(\Delta_{B/I} \otimes B/I) \circ \Delta_{B/I} \circ \pi_I &= (\Delta_{B/I} \otimes B/I) \circ (\pi_I \otimes \pi_I) \circ \Delta_B \\
&= \big((\Delta_{B/I} \circ \pi_I) \otimes \pi_I\big) \circ \Delta_B \\
&= \big(((\pi_I \otimes \pi_I) \circ \Delta_B) \otimes \pi_I\big) \circ \Delta_B \\
&= (\pi_I \otimes \pi_I \otimes \pi_I) \circ (\Delta_B \otimes B) \circ \Delta_B \\
&= (\pi_I \otimes \pi_I \otimes \pi_I) \circ (B \otimes \Delta_B) \circ \Delta_B \\
&= \big(\pi_I \otimes ((\pi_I \otimes \pi_I) \circ \Delta_B)\big) \circ \Delta_B \\
&= \big(\pi_I \otimes (\Delta_{B/I} \circ \pi_I)\big) \circ \Delta_B \\
&= (B/I \otimes \Delta_{B/I}) \circ (\pi_I \otimes \pi_I) \circ \Delta_B \\
&= (B/I \otimes \Delta_{B/I}) \circ \Delta_{B/I} \circ \pi_I
\end{aligned}$$

e

$$\begin{aligned}
(B/I \otimes \varepsilon_{B/I}) \circ \Delta_{B/I} \circ \pi_I &= (B/I \otimes \varepsilon_{B/I}) \circ (\pi_I \otimes \pi_I) \circ \Delta_B \\
&= \big(\pi_I \otimes (\varepsilon_{B/I} \circ \pi_I)\big) \circ \Delta_B \\
&= (\pi_I \otimes \varepsilon_B) \circ \Delta_B \\
&= (\pi_I \otimes \mathbb{K}) \circ (B \otimes \varepsilon_B) \circ \Delta_B \\
&= (\pi_I \otimes \mathbb{K}) \circ \tau_B \\
&= \tau_{B/I} \circ \pi_I
\end{aligned}$$

Como π_I é epimorfismo, temos que:

$$(\Delta_{B/I} \otimes B/I) \circ \Delta_{B/I} = (B/I \otimes \Delta_{B/I}) \circ \Delta_{B/I}$$

e

$$(B/I \otimes \varepsilon_{B/I}) \circ \Delta_{B/I} = \tau_{B/I}$$

À esquerda temos um resultado análogo. Portanto B/I é coálgebra. Como $\Delta_{B/I}$ e $\varepsilon_{B/I}$ são morfismos de álgebras, temos que B/I é biálgebra. Além disso, como π_I é morfismo de álgebras e:

$$(\pi_I \otimes \pi_I) \circ \Delta_B = \Delta_{B/I} \circ \pi_I$$

temos que π_I é morfismo de biálgebras. $\square$

Definição 1.49. *Seja B uma biálgebra e (M, ρ_M) um B-comódulo à direita. Um elemento $m \in M$ é dito coinvariante se:*

$$\rho_M(m) = m \otimes 1$$

Denotaremos por $M^{co\,B}$ o conjunto de todos os elementos coinvariantes de M.
Pela $\mathbb{K}$-linearidade de ρ_M, temos que $M^{co\,B}$ é um $\mathbb{K}$-submódulo de M. Como:

$$\rho_M(m) = m \otimes 1 \in M^{co\,B} \otimes C, \forall m \in M^{co\,B}$$

temos que $M^{co\,B}$ é B-subcomódulo de M.

Definição 1.50. *Seja B uma biálgebra. A biálgebra B^{op} é definida da seguinte forma:*

1) $B^{op} = B$ como K-módulo;

2) $B^{op} = B$ como coálgebra;

3) a estrutura de álgebra de B^{op} é dada por: $m_{B^{op}}(a \otimes b) = m_B(b \otimes a)$, $\forall a, b \in B$.

Definição 1.51. *Seja B uma biálgebra e $f\colon B \to B^{op}$ um morfismo de álgebras. Definimos o conjunto B^f como:*

$$B^f = \{b \in B; \sum f(b_1)b_2 = \sum b_1 f(b_2) = \varepsilon(b)1\}$$

Proposição 1.52. *Seja B uma biálgebra e $f\colon B \to B^{op}$ um morfismo de álgebras. Então B^f é uma subálgebra de B.*

Demonstração. Vejamos que $1 \in B^f$. De fato, como $\Delta(1) = 1 \otimes 1$ e $\varepsilon(1) = 1$, temos que:

$$f(1)1 = 1 = \varepsilon(1)1 = 1f(1)$$

Portanto $1 \in B^f$.
Vejamos que se $a, b \in B^f$, então $ab \in B^f$. De fato, temos:

$$\begin{aligned}
\sum f((ab)_1)(ab)_2 &= \sum f(a_1b_1)a_2b_2 \\
&= \sum f(b_1)f(a_1)a_2b_2 \\
&= \varepsilon(a) \sum f(b_1)b_2 \\
&= \varepsilon(a)\varepsilon(b)1 \\
&= \varepsilon(ab)1
\end{aligned}$$

e

$$\begin{aligned}
\sum (ab)_1 f((ab)_2) &= \sum a_1b_1 f(a_2b_2) \\
&= \sum a_1b_1 f(b_2)f(a_2) \\
&= \varepsilon(b) \sum a_1 f(a_2) \\
&= \varepsilon(b)\varepsilon(a)1 \\
&= \varepsilon(a)\varepsilon(b)1 \\
&= \varepsilon(ab)1
\end{aligned}$$

Portanto $ab \in B^f$, $\forall a, b \in B^f$.
Vejamos que se $a, b \in B^f$, então $a + b \in B^f$. De fato, como:

$$\Delta(a+b) = \Delta(a) + \Delta(b) = \sum a_1 \otimes a_2 + \sum b_1 \otimes b_2 = \sum (a_1 \otimes a_2 + b_1 \otimes b_2)$$

temos que:

$$\begin{aligned}
\sum f((a+b)_1)(a+b)_2 &= \sum (f(a_1)a_2 + f(b_1)b_2) \\
&= \varepsilon(a)1 + \varepsilon(b)1 \\
&= \varepsilon(a+b)1
\end{aligned}$$

e

$$\begin{aligned}
\sum (a+b)_1 f((a+b)_2) &= \sum (a_1 f(a_2) + b_1 f(b_2)) \\
&= \varepsilon(a)1 + \varepsilon(b)1 \\
&= \varepsilon(a+b)1
\end{aligned}$$

Portanto B^f é uma subálgebra de B. $\square$

Definição 1.53. *Sejam C uma coálgebra, A uma álgebra e $f, g\colon C \to A$ morfismos $\mathbb{K}$-lineares. Definimos o produto de convolução de f e g por:*

$$\begin{aligned} f * g\colon C &\longrightarrow A \\ c &\longmapsto \sum f(c_1)g(c_2) \end{aligned}$$

Proposição 1.54. *Sejam (C, Δ, ε) uma coálgebra e (A, m, u) uma álgebra. O conjunto $Hom(C, A)$ é uma $\mathbb{K}$-álgebra com o produto de convolução, com a unidade dada por $u \circ \varepsilon\colon C \to A$.*

Definição 1.55. *Seja H uma biálgebra. Uma função $\mathbb{K}$-linear $S\colon H \to H$ é chamada de antípoda da biálgebra H se S é a inversa da função identidade $I\colon H \to H$ com respeito ao produto de convolução em $Hom(H, H)$, ou seja, $\forall h \in H$, temos:*

$$\sum S(h_1)h_2 = \sum h_1 S(h_2) = \varepsilon(h)1$$

Definição 1.56. *Uma biálgebra H que tem antípoda é chamada de álgebra de Hopf.*

A proposição a seguir mostra as principais propriedades da antípoda, que serão utilizadas livremente ao longo deste trabalho. Sua demonstração encontra-se em [4].

Proposição 1.57. *Seja H uma álgebra de Hopf e S sua antípoda. Então para todo $h, g \in H$ temos:*

1) $S(hg) = S(g)S(h)$

2) $S(1) = 1$

3) $\Delta(S(h)) = \sum S(h_2) \otimes S(h_1)$

4) $\varepsilon(S(h)) = \varepsilon(h)$

Corolário 1.58. *Seja H uma biálgebra. Então H é uma álgebra de Hopf com antípoda S se, e somente se, $H^S = H$ para o morfismo de álgebras $S\colon H \to H^{op}$.*

O corolário acima será utilizado na Proposição 2.6 da Seção 2.1 e sua demonstração é consequência direta da Definição 1.51.

Exemplo 1.59. *Seja G um grupo e $\mathbb{K}$ um corpo. A álgebra $\mathbb{K}G$ é uma álgebra de Hopf com estrutura dada por:*

$$\begin{aligned} \Delta_{\mathbb{K}G}\colon \mathbb{K}G &\longrightarrow \mathbb{K}G \otimes \mathbb{K}G \\ h &\longmapsto h \otimes h \end{aligned}$$

$$\begin{aligned} \varepsilon_{\mathbb{K}G}\colon \mathbb{K}G &\longrightarrow \mathbb{K} \\ h &\longmapsto 1 \end{aligned}$$

e

$$\begin{aligned} S_{\mathbb{K}G}\colon \mathbb{K}G &\longrightarrow \mathbb{K}G \\ h &\longmapsto h^{-1} \end{aligned}$$

Exemplo 1.60. *O dual de $\mathbb{K}G$ dado por $(\mathbb{K}G)^* = Hom_{\mathbb{K}}(\mathbb{K}G, \mathbb{K})$ é álgebra com o produto de convolução e é álgebra de Hopf com estrutura dada por:*

$$\begin{aligned} \Delta_{(\mathbb{K}G)^*} \colon (\mathbb{K}G)^* &\longrightarrow (\mathbb{K}G)^* \otimes (\mathbb{K}G)^* \\ p_h &\longmapsto \sum_{g\in G} p_g \otimes p_{g^{-1}h} \end{aligned}$$

$$\begin{aligned} \varepsilon_{(\mathbb{K}G)^*} \colon (\mathbb{K}G)^* &\longrightarrow \mathbb{K} \\ p_h &\longmapsto \delta_{1,h} \end{aligned}$$

e

$$\begin{aligned} S_{(\mathbb{K}G)^*} \colon (\mathbb{K}G)^* &\longrightarrow (\mathbb{K}G)^* \\ p_h &\longmapsto p_{h^{-1}} \end{aligned}$$

Como $\Delta_{\mathbb{K}G}(h) = h \otimes h$, $\forall h \in G$, temos que:

$$p_g p_h := (p_g * p_h) = \delta_{g,h} p_g$$

Além disso, sabemos que a unidade em $Hom_{\mathbb{K}}(\mathbb{K}G, \mathbb{K})$ é dada por $u_{\mathbb{K}}\varepsilon_{\mathbb{K}G}$. Como $u_{\mathbb{K}}$ é a identidade em $\mathbb{K}$, temos:

$$1 = u_{\mathbb{K}}\varepsilon_{\mathbb{K}G} = \sum u_{\mathbb{K}}\varepsilon_{\mathbb{K}G}(g)p_g = \sum p_g$$

Vejamos que $(\mathbb{K}G)^*$ é coálgebra. De fato:

$$\begin{aligned} (\Delta_{(\mathbb{K}G)^*} \otimes (\mathbb{K}G)^*) \circ \Delta_{(\mathbb{K}G)^*}(p_h) &= (\Delta_{(\mathbb{K}G)^*} \otimes (\mathbb{K}G)^*)\big(\sum_{g\in G} p_g \otimes p_{g^{-1}h}\big) \\ &= \sum_{g\in G}\sum_{k\in G} p_k \otimes p_{k^{-1}g} \otimes p_{g^{-1}h} \\ &= \sum_{k\in G} p_k \otimes \big(\sum_{g\in G} p_{k^{-1}g} \otimes p_{g^{-1}kk^{-1}h}\big) \\ &= \sum_{k\in G} p_k \otimes \Delta_{(\mathbb{K}G)^*}(p_{k^{-1}h}) \\ &= ((\mathbb{K}G)^* \otimes \Delta_{(\mathbb{K}G)^*}) \circ \Delta_{(\mathbb{K}G)^*}(p_h) \end{aligned}$$

e

$$\begin{aligned} ((\mathbb{K}G)^* \otimes \varepsilon_{(\mathbb{K}G)^*}) \circ \Delta_{(\mathbb{K}G)^*}(p_h) &= ((\mathbb{K}G)^* \otimes \varepsilon_{(\mathbb{K}G)^*})\big(\sum_{g\in G} p_g \otimes p_{g^{-1}h}\big) \\ &= \sum_{g\in G} p_g \otimes \varepsilon_{(\mathbb{K}G)^*}(p_{g^{-1}h}) \\ &= p_h \otimes 1 \end{aligned}$$

Temos o resultado análogo à esquerda. Portanto $(\mathbb{K}G)^*$ é coálgebra.

Claramente $\varepsilon_{(\mathbb{K}G)^*}$ é morfismo de álgebras. Vejamos que $\Delta_{(\mathbb{K}G)^*}$ é morfismo de álgebras. De fato:

$$\begin{aligned} \Delta_{(\mathbb{K}G)^*}(p_g p_h) &= \delta_{g,h}\Delta_{(\mathbb{K}G)^*}(p_g) \\ &= \delta_{g,h}\sum_{k\in G} p_k \otimes p_{k^{-1}g} \end{aligned}$$

e

$$\begin{aligned}\Delta_{(\mathbb{K}G)^*}(p_g)\Delta_{(\mathbb{K}G)^*}(p_h) &= \big(\sum_{k\in G} p_k \otimes p_{k^{-1}g}\big)\big(\sum_{s\in G} p_s \otimes p_{s^{-1}h}\big)\\ &= \sum_{k\in G}\sum_{s\in G} p_k p_s \otimes p_{k^{-1}g}p_{s^{-1}h}\\ &= \sum_{k\in G} p_k \otimes p_{k^{-1}g}p_{k^{-1}h}\\ &= \delta_{g,h}\sum_{k\in G} p_k \otimes p_{k^{-1}g}\end{aligned}$$

Portanto $(\mathbb{K}G)^*$ *é uma biálgebra.*
Vejamos que $S_{(\mathbb{K}G)^*}$ *é a antípoda. Para cada* $h \in G$ *temos:*

$$\begin{aligned}(S_{(\mathbb{K}G)^*} * (\mathbb{K}G)^*)(p_h) &= \sum S_{(\mathbb{K}G)^*}(p_g)p_{g^{-1}h}\\ &= \sum p_{g^{-1}}p_{g^{-1}h}\end{aligned}$$

e

$$\begin{aligned}((\mathbb{K}G)^* * S_{(\mathbb{K}G)^*})(p_h) &= \sum p_g S_{(\mathbb{K}G)^*}(p_{g^{-1}h})\\ &= \sum p_g p_{h^{-1}g}\end{aligned}$$

Logo, temos que:

- *se* $h \neq 1$, *então* $p_{g^{-1}}p_{g^{-1}h} = 0 = p_g p_{h^{-1}g}$, $\forall g \in G$. *Ou seja:*

$$(S_{(\mathbb{K}G)^*} * (\mathbb{K}G)^*)(p_h) = 0 = \varepsilon(p_h)\sum p_g = ((\mathbb{K}G)^* * S_{(\mathbb{K}G)^*})(p_h)$$

- *se* $h = 1$, *então* $p_{g^{-1}}p_{g^{-1}h} = p_g^{-1}$ *e* $p_g p_{h^{-1}g} = p_g$, $\forall g \in G$. *Ou seja:*

$$(S_{(\mathbb{K}G)^*} * (\mathbb{K}G)^*)(p_h) = \sum p_g = \varepsilon(p_h)\sum p_g = ((\mathbb{K}G)^* * S_{(\mathbb{K}G)^*})(p_h)$$

Portanto $S_{(\mathbb{K}G)^*}$ *é a antípoda de* $(\mathbb{K}G)^*$.

1.6 Extensões Galois

Nesta seção apresentaremos alguns resultados de Teoria de Galois para corpos, a fim de relacionar esta teoria com a definição de extensões Galois sobre álgebras de Hopf: Seja H uma álgebra de Hopf e A um H-comódulo álgebra à direita com coação $\rho\colon A \to A \otimes H$. Dizemos que A é uma H-extensão Galois de $A^{co\,H}$ se a função:

$$\begin{aligned}\kappa_r\colon A \underset{A^{co\,H}}{\otimes} A &\longrightarrow A \otimes H\\ a \otimes b &\longmapsto a\rho(b)\end{aligned}$$

é bijetora.

Teorema 1.61. *(Dedekind). Se* $g_1, ..., g_n$ *são automorfismos de* $\mathbb{E}$ *distintos dois a dois, então são linearmente independentes sobre* $\mathbb{E}$ *como funções de* $\mathbb{E}$ *em* $\mathbb{E}$.

Lembrando que:

- o corpo $\mathbb{E}$ é uma extensão do corpo $\mathbb{F}$, denotado por $\mathbb{E}/\mathbb{F}$, se $\mathbb{F}$ é um subcorpo de $\mathbb{E}$. Denotamos por $[\mathbb{E} : \mathbb{F}]$ a dimensão de $\mathbb{E}$ sobre $\mathbb{F}$. Quando $[\mathbb{E} : \mathbb{F}] < \infty$, dizemos que a extensão é finita;
- se $\mathbb{E}/\mathbb{F}$ é uma extensão, denotaremos por $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ o subgrupo de automorfismos de $\mathbb{E}$ que fixam $\mathbb{F}$, ou seja:
$$\mathrm{Gal}(\mathbb{E}/\mathbb{F}) := \{f \in Aut(\mathbb{E}); f(a) = a, \forall a \in \mathbb{F}\}$$
- se G é um subgrupo de $\mathrm{Aut}(\mathbb{E})$, denotaremos por $\mathbb{E}^G$ o corpo fixado por G, ou seja:
$$\mathbb{E}^G := \{a \in \mathbb{E}; g(a) = a, \forall g \in G\}$$
- se $\mathbb{E}/\mathbb{F}$ é uma extensão finita, diremos que a extensão é Galois se $\mathbb{F} = \mathbb{E}^{\mathrm{Gal}(\mathbb{E}/\mathbb{F})}$.

Teorema 1.62. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão finita. Então a extensão é Galois se, e somente se, $|Gal(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}]$.*

Demonstração. A demonstração completa pode ser encontrada em [11]. Mostraremos apenas que:
$$|\mathrm{Gal}(\mathbb{E}/\mathbb{F})| \leq [\mathbb{E} : \mathbb{F}]$$

Suponha por absurdo que:
$$m = |\mathrm{Gal}(\mathbb{E}/\mathbb{F})| > [\mathbb{E} : \mathbb{F}] = n$$

Sejam $\{e_1, ..., e_n\}$ uma base de $\mathbb{E}/\mathbb{F}$ e $G = \{g_1, ..., g_m\}$. Então o sistema abaixo possui solução não trivial:
$$\begin{bmatrix} x_1 & \cdots & x_m \end{bmatrix} \begin{bmatrix} g_1(e_1) & \cdots & g_1(e_n) \\ \vdots & \ddots & \vdots \\ g_m(e_1) & \cdots & g_m(e_n) \end{bmatrix} = 0$$

Ou seja, existem $b_1, ..., b_n$ não todos nulos tais que, para todo i:
$$\sum b_j g_j(e_i) = 0$$
o que implica que:
$$\sum b_j g_j = 0$$

Absurdo, pois pelo teorema 1.61, temos que $G = \{g_1, ..., g_n\}$ é um conjunto linearmente independente. Portanto:
$$|\mathrm{Gal}(\mathbb{E}/\mathbb{F})| \leq [\mathbb{E} : \mathbb{F}]$$

□

Definição 1.63. *Sejam A um conjunto e $\mathbb{K}$ um corpo. Denotaremos por $\mathcal{F}(A, \mathbb{K})$ o $\mathbb{K}$-espaço vetorial das funções de A para $\mathbb{K}$, com:*
$$(f + \lambda g)(a) = f(a) + \lambda g(a),\ \forall f, g \in \mathcal{F}(A, \mathbb{K}),\ \forall \lambda \in \mathbb{K},\ \forall a \in A$$

Teorema 1.64. *Sejam $\mathbb{E}/\mathbb{F}$ uma extensão finita e $G = Gal(\mathbb{E}/\mathbb{F})$. Então $\mathbb{E}/\mathbb{F}$ é Galois se, e somente se, a função:*
$$\begin{aligned} \phi\colon \mathbb{E} \underset{\mathbb{F}}{\otimes} \mathbb{E} &\longrightarrow \mathcal{F}(G, \mathbb{E}) \\ a \otimes b &\longmapsto \big(g \mapsto a g(b)\big) \end{aligned}$$

é bijetora.

Demonstração. ($\Rightarrow$) Se $\mathbb{E}/\mathbb{F}$ é Galois, então $[\mathbb{E}:\mathbb{F}] = |G|$. Além disso, temos que:

$$\dim_{\mathbb{E}}(\mathbb{E} \underset{\mathbb{F}}{\otimes} \mathbb{E}) = [\mathbb{E}:\mathbb{F}]$$

e

$$\dim_{\mathbb{E}}(\mathcal{F}(G,\mathbb{E})) = |G|$$

Logo, temos que:

$$\dim_{\mathbb{E}}(\mathbb{E} \underset{\mathbb{F}}{\otimes} \mathbb{E}) = \dim_{\mathbb{E}}(\mathcal{F}(G,\mathbb{E}))$$

Vejamos que ϕ é injetora. De fato, sejam $\{e_1, ..., e_n\}$ uma base de $\mathbb{E}/\mathbb{F}$ e $G = \{g_1, ..., g_n\}$. Suponha por absurdo que existe $0 \neq \sum a_i \otimes e_i \in \ker\phi$. Então para cada $g_j \in G$, temos:

$$\sum a_i g_j(e_i) = 0$$

Equivalentemente, temos que o sistema abaixo tem solução não trivial:

$$\begin{bmatrix} g_1(e_1) & \cdots & g_1(e_n) \\ \vdots & \ddots & \vdots \\ g_n(e_1) & \cdots & g_n(e_n) \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = 0$$

Portanto a matriz:

$$\begin{bmatrix} g_1(e_1) & \cdots & g_1(e_n) \\ \vdots & \ddots & \vdots \\ g_n(e_1) & \cdots & g_n(e_n) \end{bmatrix}$$

é singular. Logo o sistema abaixo possui uma solução não trivial:

$$\begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix} \begin{bmatrix} g_1(e_1) & \cdots & g_1(e_n) \\ \vdots & \ddots & \vdots \\ g_n(e_1) & \cdots & g_n(e_n) \end{bmatrix} = 0$$

Ou seja, existem $b_1, ..., b_n$ não todos nulos tais que, para todo i:

$$\sum b_j g_j(e_i) = 0$$

o que implica que:

$$\sum b_j g_j = 0$$

Absurdo, pois pelo teorema 1.61, temos que $G = \{g_1, ..., g_n\}$ é um conjunto linearmente independente. Portanto $\ker\phi = 0$ e ϕ é injetora. Como:

$$\dim_{\mathbb{E}}(\mathbb{E} \underset{\mathbb{F}}{\otimes} \mathbb{E}) = \dim_{\mathbb{E}}(\mathcal{F}(G,\mathbb{E}))$$

temos que ϕ é bijetora.

($\Leftarrow$) Se ϕ é bijetora, então:

$$\begin{aligned} [\mathbb{E}:\mathbb{F}] &= \dim_{\mathbb{E}}(\mathbb{E} \underset{\mathbb{F}}{\otimes} \mathbb{E}) \\ &= \dim_{\mathbb{E}}(\mathcal{F}(G,\mathbb{E})) \\ &= |G| \\ &= \left[\mathbb{E}:\mathbb{E}^G\right] \end{aligned}$$

Como $\mathbb{F} \subset \mathbb{E}^G$, temos que $[\mathbb{E}:\mathbb{F}] = \left[\mathbb{E}:\mathbb{E}^G\right]\left[\mathbb{E}^G:\mathbb{F}\right]$.

Portanto $\left[\mathbb{E}^G:\mathbb{F}\right] = 1$ e $\mathbb{F} = \mathbb{E}^G$, ou seja, $\mathbb{E}/\mathbb{F}$ é Galois. $\square$

Proposição 1.65. *Sejam $\mathbb{E}/\mathbb{F}$ uma extensão finita, $G \subset Gal(\mathbb{E}/\mathbb{F})$ e $\mathbb{K}$ um subcorpo de $\mathbb{F}$. Então a função:*

$$\begin{aligned} \varphi\colon \mathcal{F}(G,\mathbb{E}) &\longrightarrow \mathbb{E} \underset{\mathbb{K}}{\otimes} (\mathbb{K}G)^* \\ f &\longmapsto \sum_{g\in G} f(g)\otimes p_g \end{aligned}$$

é bijetora, onde $\{p_g\}_{g\in G}$ é base de $(\mathbb{K}G)^*$ sobre $\mathbb{K}$.

Demonstração. Temos que:

$$\begin{aligned} \dim_{\mathbb{E}}(\mathcal{F}(G,\mathbb{E})) &= |G| \\ &= \dim_{\mathbb{E}}(\mathbb{E}\otimes(\mathbb{K}G)^*) \end{aligned}$$

Logo, para verificar que φ é bijetora, é suficiente verificar que é injetora. Seja $f \in \ker\varphi$. Então:

$$\sum_{g\in G} f(g)\otimes p_g = 0$$

Pela independência linear de $\{p_g\}$ em $(\mathbb{K}G)^*$, temos que $\{1\otimes p_g\}$ é linearmente independente em $\mathbb{E}\otimes(\mathbb{K}G)^*$ sobre $\mathbb{E}$, o que implica que $\forall g\in G$:

$$f(g) = 0$$

Portanto $f \equiv 0$ e φ é injetora. □

A partir dos dois últimos resultados, temos o seguinte teorema:

Teorema 1.66. *Sejam $\mathbb{E}/\mathbb{F}$ uma extensão finita, $G = Gal(\mathbb{E}/\mathbb{F})$ e $\mathbb{K}$ um subcorpo de $\mathbb{F}$. Então a extensão é Galois se, e somente se, a função:*

$$\begin{aligned} \kappa_r\colon \mathbb{E}\underset{\mathbb{F}}{\otimes}\mathbb{E} &\longrightarrow \mathbb{E} \underset{\mathbb{K}}{\otimes} (\mathbb{K}G)^* \\ a\otimes b &\longmapsto \sum a\, g(b)\otimes p_g \end{aligned}$$

é bijetora.

A partir da estrutura acima, podemos definir:

$$\begin{aligned} \rho\colon \mathbb{E} &\longrightarrow \mathbb{E}\otimes(\mathbb{K}G)^* \\ b &\longmapsto \sum g(b)\otimes p_g \end{aligned}$$

Proposição 1.67. *O espaço $\mathbb{E}$ é $(\mathbb{K}G)^*$-comódulo com ρ dado acima, e $\mathbb{E}^G = \mathbb{E}^{co\,(\mathbb{K}G)^*}$.*

Demonstração. Precisamos verificar que os seguintes diagramas comutam:

$$\begin{tikzcd} \mathbb{E} \arrow[r, "\rho"] \arrow[d, "\rho"'] & \mathbb{E}\otimes(\mathbb{K}G)^* \arrow[d, "\rho\otimes(\mathbb{K}G)^*"] \\ \mathbb{E}\otimes(\mathbb{K}G)^* \arrow[r, "\mathbb{E}\otimes\Delta_{(\mathbb{K}G)^*}"] & \mathbb{E}\otimes(\mathbb{K}G)^*\otimes(\mathbb{K}G)^* \end{tikzcd}$$

$$\begin{tikzcd} \mathbb{E} \arrow[rr, "\rho"] \arrow[dr, "\cong"'] & & \mathbb{E}\otimes(\mathbb{K}G)^* \arrow[dl, "\mathbb{E}\otimes\varepsilon_{(\mathbb{K}G)^*}"] \\ & \mathbb{E}\otimes\mathbb{K} & \end{tikzcd}$$

De fato, para cada $b \in \mathbb{E}$, temos:

$$\begin{aligned}(\rho \otimes (\mathbb{K}G)^*) \circ \rho(b) &= (\rho \otimes (\mathbb{K}G)^*)\big(\sum g(b) \otimes p_g\big)\\ &= \sum h(g(b)) \otimes p_h \otimes p_g\\ &= \sum k(b) \otimes \big(\sum p_g \otimes p_{g^{-1}k}\big)\\ &= (\mathbb{E} \otimes \Delta_{(\mathbb{K}G)^*})\big(\sum k(b) \otimes p_k\big)\\ &= (\mathbb{E} \otimes \Delta_{(\mathbb{K}G)^*}) \circ \rho(b)\end{aligned}$$

e

$$\begin{aligned}(\mathbb{E} \otimes \varepsilon_{(\mathbb{K}G)^*}) \circ \rho(b) &= (\mathbb{E} \otimes \varepsilon_{(\mathbb{K}G)^*})\big(\sum g(b) \otimes p_g\big)\\ &= \sum g(b) \otimes \varepsilon_{(\mathbb{K}G)^*}(p_g)\\ &= 1(b) \otimes 1\\ &= b \otimes 1\end{aligned}$$

Portanto $\mathbb{E}$ é $(\mathbb{K}G)^*$-comódulo.
Vejamos que $\mathbb{E}^G = \mathbb{E}^{co\,(\mathbb{K}G)^*}$. De fato, temos que:

$$b \in \mathbb{E}^G \iff g(b) = b, \forall g \in G$$

Como $\{1 \otimes p_g\}$ é base de $\mathbb{E} \otimes (\mathbb{K}G)^*$, temos que:

$$g(b) = b, \forall g \in G \iff \sum g(b) \otimes p_g = \sum b \otimes p_g = b \otimes \big(\sum p_g\big)$$

Como $\big(\sum p_g\big) = 1$ em $(\mathbb{K}G)^*$, temos que:

$$\sum g(b) \otimes p_g = b \otimes \big(\sum p_g\big) \iff b \in \mathbb{E}^{co\,(\mathbb{K}G)^*}$$

Portanto:

$$b \in \mathbb{E}^G \iff b \in \mathbb{E}^{co\,(\mathbb{K}G)^*}$$

□

1.7 Extensões Galois sobre Álgebras de Hopf

Nesta seção apresentaremos as extensões Galois sobre álgebras de Hopf, bem como uma caracterização dos objetos H-Galois através de funtores monoidais e explicaremos como o produto cotensorial dá uma estrutura de grupo para a classe dos objetos H-biGalois fielmente $\mathbb{K}$-planos.

Definição 1.68. *Sejam H uma álgebra de Hopf e $B \subset A$ álgebras. Diremos que A é uma H-extensão à direita (à esquerda) de B se A é um H-comódulo álgebra à direita (à esquerda) e $B = A^{co\,H}$.*

A partir deste ponto, quando não houver menção dos termos "à direita"ou "à esquerda", assumiremos a estrutura à direita. Todos os resultados apresentados possuem o seu análogo à esquerda.

Definição 1.69. *Sejam A_1 e A_2 duas H-extensões de B. Diremos que uma função:*

$$T\colon A_1 \longrightarrow A_2$$

é um morfismo de H-extensões de B se T é morfismo de H-comódulo álgebras e $T(b) = b$, $\forall b \in B$.

Definição 1.70. *Sejam H uma álgebra de Hopf e A uma H-extensão B. Dizemos que A é uma H-extensão Galois de B se a função A-linear à esquerda e H-colinear à direita:*

$$\begin{aligned} \kappa_r\colon A \underset{B}{\otimes} A &\longrightarrow A \otimes H \\ a \otimes b &\longmapsto a\rho_A(b) = \sum ab_{(0)} \otimes b_{(1)} \end{aligned}$$

é um isomorfismo. Chamaremos κ_r de função canônica de A.

Quando $B \cong \mathbb{K}$, dizemos que A é um objeto H-Galois à direita.

Nos resultados a seguir, usaremos a definição de categoria monoidal e funtor monoidal dadas por Saunders Mac Lane em [12] e descritas no Apêndice D.

Lembrando que, na notação de Sweedler, temos:

- Se C é uma coálgebra, então para cada $c \in C$ denotaremos:

$$\Delta_C(c) = \sum c_1 \otimes c_2$$

- Se (M, β_M) é um C-comódulo à esquerda, então para cada $m \in M$ denotaremos:

$$\rho_M(m) = \sum m_{(-1)} \otimes m_{(0)}$$

  Como temos que $(C \otimes \beta_M) \circ \beta_M = (\Delta_C \otimes M) \circ \beta_M$, podemos estender esta notação da seguinte forma:

$$\sum m_{(-2)} \otimes m_{(-1)} \otimes m_{(0)} := \sum m_{(-1)} \otimes m_{(0),(-1)} \otimes m_{(0),(0)} = \sum m_{(-1),1} \otimes m_{(-1),2} \otimes m_{(0)}$$

Proposição 1.71. *Seja H uma biálgebra. A categoria dos H-comódulos à esquerda é uma categoria monoidal com:*

$$\begin{aligned} \otimes\colon {}^H\mathcal{M} \times {}^H\mathcal{M} &\longrightarrow {}^H\mathcal{M} \\ M \times N &\longmapsto M \otimes N \end{aligned}$$

onde $M \otimes N$ é H-comódulo com estrutura dada por:

$$\beta_{M\otimes N}(m \otimes n) = \sum m_{(-1)}n_{(-1)} \otimes m_{(0)} \otimes n_{(0)}$$

e isomorfismos naturais para cada $M, N, S \in {}^H\mathcal{M}$ dados por:

$$\begin{aligned} \varpi\colon M \otimes (N \otimes S) &\longrightarrow (M \otimes N) \otimes S \\ m \otimes n \otimes s &\longmapsto m \otimes n \otimes s \end{aligned}$$

$$\begin{aligned} \omega^l_M\colon \mathbb{K} \otimes M &\longrightarrow M \\ \lambda \otimes m &\longmapsto \lambda m \end{aligned}$$

e

$$\begin{aligned} \omega^r_M\colon M \otimes \mathbb{K} &\longrightarrow M \\ m \otimes \lambda &\longmapsto \lambda m \end{aligned}$$

Demonstração. Precisamos verificar que os seguintes diagramas comutam:

$$\begin{tikzcd}
M \otimes N \arrow[r, "\beta_{M\otimes N}"] \arrow[d, "\beta_{M\otimes N}"'] & H \otimes M \otimes N \arrow[d, "H\otimes\beta_{M\otimes N}"] \\
H \otimes M \otimes N \arrow[r, "\Delta_H\otimes M\otimes N"] & H \otimes H \otimes M \otimes N
\end{tikzcd}$$

$$\begin{tikzcd}
M \otimes N \arrow[rr, "\beta_{M\otimes N}"] \arrow[dr, "\cong"'] & & H \otimes M \otimes N \arrow[dl, "\varepsilon_H\otimes M\otimes N"] \\
& \mathbb{K} \otimes M \otimes N &
\end{tikzcd}$$

De fato, $\forall m \in M$ e $n \in N$ temos:

$$\begin{aligned}
(H \otimes \beta_{M\otimes N}) \circ \beta_{M\otimes N}(m \otimes n) &= (H \otimes \beta_{M\otimes N})\left(\sum m_{(-1)}n_{(-1)} \otimes m_{(0)} \otimes n_{(0)}\right) \\
&= \sum m_{(-1)}n_{(-1)} \otimes m_{(0),(-1)}n_{(0),(-1)} \otimes m_{(0),(0)} \otimes n_{(0),(0)} \\
&= \sum m_{(-1),1}n_{(-1),1} \otimes m_{(-1),2}n_{(-1),2} \otimes m_{(0)} \otimes n_{(0)} \\
&= (\Delta_H \otimes M \otimes N)(m_{(-1)}n_{(-1)} \otimes m_{(0)} \otimes n_{(0)}) \\
&= (\Delta_H \otimes M \otimes N) \circ \beta_{M\otimes N}(m \otimes n)
\end{aligned}$$

e

$$\begin{aligned}
(\varepsilon_H \otimes M \otimes N) \circ \beta_{M\otimes N}(m \otimes n) &= (\varepsilon_H \otimes M \otimes N)\left(\sum m_{(-1)}n_{(-1)} \otimes m_{(0)} \otimes n_{(0)}\right) \\
&= \sum \varepsilon_H(m_{(-1)}n_{(-1)}) \otimes m_{(0)} \otimes n_{(0)} \\
&= \sum \varepsilon_H(m_{(-1)})\varepsilon_H(n_{(-1)}) \otimes m_{(0)} \otimes n_{(0)} \\
&= \sum 1 \otimes \varepsilon_H(m_{(-1)})m_{(0)} \otimes \varepsilon_H(n_{(-1)})n_{(0)} \\
&= 1 \otimes m \otimes n
\end{aligned}$$

Portanto $M \otimes N$ é H-comódulo à esquerda.

Claramente, usando elementos, os diagramas para categoria monoidal comutam. □

Definição 1.72. *Seja $\mathcal{F}\colon \mathcal{M}_{\mathbb{K}} \to \mathcal{M}_{\mathbb{K}}$ um funtor. Diremos que $\mathcal{F}$ é fielmente exato se a sequência:*

$$0 \longrightarrow V \xrightarrow{f} W \xrightarrow{g} Z \longrightarrow 0$$

é exata se, e somente se, a sequência:

$$0 \longrightarrow \mathcal{F}(V) \xrightarrow{\mathcal{F}(f)} \mathcal{F}(W) \xrightarrow{\mathcal{F}(g)} \mathcal{F}(Z) \longrightarrow 0$$

é exata.

Proposição 1.73. *Sejam H uma biálgebra e $A \in \mathcal{M}^H$. Se (A, ρ_A) é H-comódulo álgebra, então:*

$$\begin{aligned}
\xi\colon (A \underset{H}{\square} V) \otimes (A \underset{H}{\square} W) &\longrightarrow A \underset{H}{\square} (V \otimes W) \\
(x \otimes v) \otimes (y \otimes w) &\longmapsto xy \otimes v \otimes w
\end{aligned}$$

e

$$\begin{aligned}
\xi_0\colon \mathbb{K} &\longrightarrow A \underset{H}{\square} \mathbb{K} \\
\alpha &\longmapsto 1 \otimes \alpha
\end{aligned}$$

definem uma estrutura de funtor monoidal fraco para $(A \underset{H}{\square} \_)\colon {}^H\mathcal{M} \to \mathcal{M}_{\mathbb{K}}$.

O H-comódulo álgebra A é (fielmente) H-coplano se, e somente se, o funtor é (fielmente) exato.

Todo funtor exato monoidal fraco ${}^H\mathcal{M} \to \mathcal{M}_{\mathbb{K}}$ tem a estrutura acima para um único H-comódulo álgebra à direita A.

Demonstração. Pela Proposição 1.39, temos que $(A \underset{H}{\square} \_)$ é um funtor.

Considere o morfismo:

$$\begin{aligned}\xi' \colon (A \underset{H}{\square} V) \otimes (A \underset{H}{\square} W) &\longrightarrow A \otimes (V \otimes W)\\ (x \otimes v) \otimes (y \otimes w) &\longmapsto xy \otimes v \otimes w\end{aligned}$$

Então temos:

$$\begin{aligned}(\rho_A \otimes V \otimes W)\xi'(x \otimes v \otimes y \otimes w) &= (\rho_A \otimes V \otimes W)(xy \otimes v \otimes w)\\ &= \rho_A(xy) \otimes v \otimes w\\ &= \sum (xy)_{(0)} \otimes (xy)_{(1)} \otimes v \otimes w\\ &= \sum \big(x_{(0)} \otimes x_{(1)} \otimes v \otimes 1\big)\big(y_{(0)} \otimes y_{(1)} \otimes 1 \otimes w\big)\\ &= \sum \big(x \otimes v_{(-1)} \otimes v_{(0)} \otimes 1\big)\big(y \otimes w_{(-1)} \otimes 1 \otimes w_{(0)}\big)\\ &= \sum xy \otimes v_{(-1)}w_{(-1)} \otimes v_{(0)} \otimes w_{(0)}\\ &= (A \otimes \beta_{V\otimes W})(xy \otimes v \otimes w)\\ &= (A \otimes \beta_{V\otimes W})\xi'(x \otimes v \otimes y \otimes w)\end{aligned}$$

Pela definição de equalizador, $\xi'\big((A \underset{H}{\square} V) \otimes (A \underset{H}{\square} W)\big) \subset A \underset{H}{\square} (V \otimes W)$. Tome:

$$\begin{aligned}\xi \colon (A \underset{H}{\square} V) \otimes (A \underset{H}{\square} W) &\longrightarrow A \underset{H}{\square} (V \otimes W)\\ x \otimes v \otimes y \otimes w &\longmapsto \xi'(x \otimes v \otimes y \otimes w)\end{aligned}$$

Considere o morfismo:

$$\begin{aligned}\xi_0' \colon \mathbb{K} &\longrightarrow A \otimes \mathbb{K}\\ \alpha &\longmapsto 1 \otimes \alpha\end{aligned}$$

Então temos:

$$\begin{aligned}(\rho_A \otimes \mathbb{K})\xi_0'(\alpha) &= \alpha(\rho_A \otimes \mathbb{K})\xi_0'(1)\\ &= \alpha(\rho_A \otimes \mathbb{K})(1 \otimes 1)\\ &= \alpha(\rho_A(1) \otimes 1)\\ &= \alpha(1 \otimes 1 \otimes 1)\\ &= \alpha(A \otimes \beta_{\mathbb{K}})(1 \otimes 1)\\ &= \alpha(A \otimes \beta_{\mathbb{K}})\xi_0'(1)\\ &= (A \otimes \beta_{\mathbb{K}})\xi_0'(\alpha)\end{aligned}$$

Pela definição de equalizador, $\xi_0'(\mathbb{K}) \subset A \underset{H}{\square} \mathbb{K}$. Tome:

$$\begin{aligned}\xi_0 \colon \mathbb{K} &\longrightarrow A \underset{H}{\square} \mathbb{K}\\ \alpha &\longmapsto \xi_0'(\alpha)\end{aligned}$$

Claramente, por elementos, os seguintes diagramas comutam:

$$\begin{tikzcd}
A\underset{H}{\square}V \otimes (A\underset{H}{\square}W \otimes A\underset{H}{\square}Z) \arrow[r, "\varpi"] \arrow[d, "A\underset{H}{\square}V\otimes\xi"'] & (A\underset{H}{\square}V \otimes A\underset{H}{\square}W) \otimes A\underset{H}{\square}Z \arrow[d, "\xi\otimes A\underset{H}{\square}Z"] \\
A\underset{H}{\square}V \otimes A\underset{H}{\square}(W\otimes Z) \arrow[d, "\xi"'] & A\underset{H}{\square}(V\otimes W) \otimes A\underset{H}{\square}Z \arrow[d, "\xi"] \\
A\underset{H}{\square}(V\otimes (W\otimes Z)) \arrow[r, "A\underset{H}{\square}\varpi"] & A\underset{H}{\square}((V\otimes W)\otimes Z)
\end{tikzcd}$$

$$\begin{tikzcd}
\mathbb{K}\otimes A\underset{H}{\square}V \arrow[r, "\omega^l_{A\underset{H}{\square}V}"] \arrow[d, "\xi_0\otimes A\underset{H}{\square}V"'] & A\underset{H}{\square}V \\
A\underset{H}{\square}\mathbb{K}\otimes A\underset{H}{\square}V \arrow[r, "\xi"] & A\underset{H}{\square}(\mathbb{K}\otimes V) \arrow[u, "A\underset{H}{\square}\omega^l_V"']
\end{tikzcd}
\qquad
\begin{tikzcd}
A\underset{H}{\square}V\otimes \mathbb{K} \arrow[r, "\omega^r_{A\underset{H}{\square}V}"] \arrow[d, "A\underset{H}{\square}V\otimes\xi_0"'] & A\underset{H}{\square}V \\
A\underset{H}{\square}V\otimes A\underset{H}{\square}\mathbb{K} \arrow[r, "\xi"] & A\underset{H}{\square}(V\otimes\mathbb{K}) \arrow[u, "A\underset{H}{\square}\omega^r_V"']
\end{tikzcd}$$

Portanto $(A\underset{H}{\square}\_)$ é funtor monoidal fraco.

Pela definição de H-coplano, A é (fielmente) H-coplano se, e somente se, $(A\underset{H}{\square}\_)$ é (fielmente) exato.

Reciprocamente, seja $\mathcal{F}\colon {}^H\mathcal{M} \to \mathcal{M}_{\mathbb{K}}$ um funtor exato monoidal fraco. Pelo Teorema 1.43, $\mathcal{F} \cong (A\underset{H}{\square}\_)$ para algum H-comódulo H-coplano A. Seja a estrutura de funtor monoidal fraco dada por:

$$\xi\colon (A\underset{H}{\square}V)\otimes(A\underset{H}{\square}W) \longrightarrow A\underset{H}{\square}(V\otimes W)$$

e

$$\xi_0\colon \mathbb{K} \longrightarrow A\underset{H}{\square}\mathbb{K}$$

e $m\colon H\otimes H \to H$ a multiplicação de H. Pela Proposição 1.37, $\rho_A\colon A \to A\underset{H}{\square}H$ é isomorfismo. Defina a multiplicação de A pela composição:

$$A\otimes A \overset{\rho_A\otimes\rho_A}{\longrightarrow} (A\underset{H}{\square}H)\otimes(A\underset{H}{\square}H) \overset{\xi}{\longrightarrow} A\underset{H}{\square}(H\otimes H) \overset{A\underset{H}{\square}m}{\longrightarrow} A\underset{H}{\square}H \overset{\rho_A^{-1}}{\longrightarrow} A$$

Vejamos que a multiplicação é associativa. Considere o isomorfismo:

$$\begin{aligned}\varpi\colon V\otimes(W\otimes Z) &\longrightarrow (V\otimes W)\otimes Z\\ v\otimes w\otimes z &\longmapsto v\otimes w\otimes z\end{aligned}$$

Identificando A com $A\underset{H}{\square}H$ pelo isomorfismo f, basta mostrar que o seguinte diagrama comuta:

$$\begin{tikzcd}
A\underset{H}{\square}H\otimes(A\underset{H}{\square}H\otimes A\underset{H}{\square}H) \arrow[r, "\varpi"] \arrow[d, "A\underset{H}{\square}H\otimes\xi"'] & (A\underset{H}{\square}H\otimes A\underset{H}{\square}H)\otimes A\underset{H}{\square}H \arrow[r, "\xi\otimes A\underset{H}{\square}H"] & A\underset{H}{\square}(H\otimes H)\otimes A\underset{H}{\square}H \arrow[r, "A\underset{H}{\square}m\otimes A\underset{H}{\square}H"] & A\underset{H}{\square}H\otimes A\underset{H}{\square}H \arrow[d, "\xi"] \\
A\underset{H}{\square}H\otimes A\underset{H}{\square}(H\otimes H) \arrow[d, "A\underset{H}{\square}H\otimes A\underset{H}{\square}m"'] & & & A\underset{H}{\square}(H\otimes H) \arrow[d, "A\underset{H}{\square}m"] \\
A\underset{H}{\square}H\otimes A\underset{H}{\square}H \arrow[r, "\xi"] & A\underset{H}{\square}(H\otimes H) \arrow[rr, "A\underset{H}{\square}m"] & & A\underset{H}{\square}H
\end{tikzcd}$$

Equivalentemente, basta mostrar que cada um dos seguintes subdiagramas comutam:

$$\begin{tikzcd}
A\underset{H}{\square}H \otimes (A\underset{H}{\square}H \otimes A\underset{H}{\square}H) \arrow[r, "\varpi"] \arrow[d, "A\underset{H}{\square}H\otimes\xi"'] & (A\underset{H}{\square}H \otimes A\underset{H}{\square}H) \otimes A\underset{H}{\square}H \arrow[r, "\xi\otimes A\underset{H}{\square}H"] & A\underset{H}{\square}(H\otimes H) \otimes A\underset{H}{\square}H \arrow[r, "A\underset{H}{\square}m\otimes A\underset{H}{\square}H"] \arrow[d, "\xi"] & A\underset{H}{\square}H \otimes A\underset{H}{\square}H \arrow[d, "\xi"] \\
A\underset{H}{\square}H \otimes A\underset{H}{\square}(H\otimes H) \arrow[r, "\xi"] \arrow[d, "A\underset{H}{\square}H\otimes A\underset{H}{\square}m"'] & A\underset{H}{\square}(H\otimes(H\otimes H)) \arrow[r, "A\underset{H}{\square}\varpi"] \arrow[d, "A\underset{H}{\square}H\otimes m"] & A\underset{H}{\square}((H\otimes H)\otimes H) \arrow[r, "A\underset{H}{\square}m\otimes H"] & A\underset{H}{\square}(H\otimes H) \arrow[d, "A\underset{H}{\square}m"] \\
A\underset{H}{\square}H \otimes A\underset{H}{\square}H \arrow[r, "\xi"] & A\underset{H}{\square}(H\otimes H) \arrow[rr, "A\underset{H}{\square}m"] & & A\underset{H}{\square}H
\end{tikzcd}$$

Como ξ dá estrutura de funtor monoidal fraco, temos:

$$(A\underset{H}{\square}\varpi) \circ \xi \circ (A\underset{H}{\square}H \otimes \xi) = \xi \circ (\xi \otimes A\underset{H}{\square}H) \circ \varpi$$

Claramente, usando elementos, temos o seguinte:

$$(A\underset{H}{\square}m) \circ (A\underset{H}{\square}m \otimes H) \circ (A\underset{H}{\square}\varpi) = (A\underset{H}{\square}m) \circ (A\underset{H}{\square}H \otimes m)$$

Além disso, ξ é transformação natural, o que implica que:

$$(A\underset{H}{\square}H \otimes m) \circ \xi = \xi \circ (A\underset{H}{\square}H \otimes A\underset{H}{\square}m)$$

e

$$(A\underset{H}{\square}m \otimes H) \circ \xi = \xi \circ (A\underset{H}{\square}m \otimes A\underset{H}{\square}H)$$

Portanto A é uma álgebra.

Não provaremos, mas é possível verificar que:

$$\rho_A(ab) = \rho_A(a)\rho_A(b)$$
$$\rho_A(1) = 1$$

□

Para a descrição dos objetos H-Galois fielmente $\mathbb{K}$-planos, precisamos de um resultado sobre a inversa da função canônica κ_r.

Observação 1.74. *Seja A uma H-extensão Galois de B. Como κ_r é isomorfismo, denotaremos a inversa de κ_r por:*

$$\kappa_r^{-1} \colon A \otimes H \longrightarrow A \underset{B}{\otimes} A$$
$$a \otimes h \longmapsto \sum ah^{[1]} \otimes h^{[2]}$$

que também é A-linear à esquerda.

Lema 1.75. *Seja A uma H-extensão Galois de B. Então para cada $a \in A$ temos:*

$$\sum a_{(0)}a_{(1)}^{[1]} \otimes a_{(1)}^{[2]} = 1 \otimes a$$

em $A \underset{B}{\otimes} A$.

Demonstração. Aplicando κ_r, temos:

$$\begin{aligned}
\kappa_r(\sum a_{(0)}a_{(1)}^{[1]} \otimes a_{(1)}^{[2]}) &= \kappa_r \circ \kappa_r^{-1}(\sum a_{(0)} \otimes a_{(1)}) \\
&= \sum a_{(0)} \otimes a_{(1)} \\
&= \kappa_r(1 \otimes a)
\end{aligned}$$

Como κ_r é isomorfismo, temos que

$$\sum a_{(0)}a_{(1)}^{[1]} \otimes a_{(1)}^{[2]} = 1 \otimes a$$

□

Lema 1.76. *Sejam H uma álgebra de Hopf e A um objeto H-Galois à direita. Então A é fielmente $\mathbb{K}$-plano se, e somente se, é fielmente H-coplano.*

Demonstração. ($\Rightarrow$) Como A é fielmente $\mathbb{K}$-plano, temos que a sequência:

$$0 \longrightarrow U \xrightarrow{f} V \xrightarrow{g} W \longrightarrow 0$$

em ${}^H\mathcal{M}$ é exata se, e somente se, a seguinte sequência:

$$0 \longrightarrow A \otimes U \xrightarrow{A\otimes f} A \otimes V \xrightarrow{A\otimes g} A \otimes W \longrightarrow 0$$

em $\mathcal{M}_{\mathbb{K}}$ é exata.

Pela Proposição 1.37, temos que $\beta_U : U \to H \underset{H}{\square} U$, $\beta_V : V \to H \underset{H}{\square} V$ e $\beta_W : W \to H \underset{H}{\square} W$ são isomorfismos. Como f e g são morfismos de H-comódulos, os seguintes diagramas comutam:

$$\begin{tikzcd} U \arrow[r, "f"] \arrow[d, "\beta_U"'] & V \arrow[d, "\beta_V"] \\ H \otimes U \arrow[r, "H\otimes f"] & H \otimes V \end{tikzcd} \qquad \begin{tikzcd} V \arrow[r, "g"] \arrow[d, "\beta_V"'] & W \arrow[d, "\beta_W"] \\ H \otimes V \arrow[r, "H\otimes g"] & H \otimes W \end{tikzcd}$$

Além disso, A é um objeto H-Galois. Logo a função canônica $\kappa : A \otimes A \to A \otimes H$ é um isomorfismo. Considere a sua inversa $\kappa^{-1} : A \otimes H \to A \otimes A$. Temos que o seguinte diagrama comuta:

$$\begin{tikzcd} 0 \arrow[r] & A \otimes U \arrow[r, "A\otimes f"] \arrow[d, "A\otimes\beta_U"'] & A \otimes V \arrow[r, "A\otimes g"] \arrow[d, "A\otimes\beta_V"] & A \otimes W \arrow[r] \arrow[d, "A\otimes\beta_W"] & 0 \\ 0 \arrow[r] & A \otimes H \underset{H}{\square} U \arrow[r, "A\otimes H\underset{H}{\square} f"] \arrow[d, "\kappa^{-1}\underset{H}{\square} U"'] & A \otimes H \underset{H}{\square} V \arrow[r, "A\otimes H\underset{H}{\square} g"] \arrow[d, "\kappa^{-1}\underset{H}{\square} V"] & A \otimes H \underset{H}{\square} W \arrow[r] \arrow[d, "\kappa^{-1}\underset{H}{\square} W"] & 0 \\ 0 \arrow[r] & A \otimes A \underset{H}{\square} U \arrow[r, "A\otimes A\underset{H}{\square} f"] & A \otimes A \underset{H}{\square} V \arrow[r, "A\otimes A\underset{H}{\square} g"] & A \otimes A \underset{H}{\square} W \arrow[r] & 0 \end{tikzcd}$$

Como temos isomorfismos nas colunas, a primeira linha é exata se, e somente se, a última linha é exata.

Mas A é fielmente $\mathbb{K}$-plano, o que implica que a sequência:

$$0 \longrightarrow A \otimes A \underset{H}{\square} U \xrightarrow{A\otimes A\underset{H}{\square} f} A \otimes A \underset{H}{\square} V \xrightarrow{A\otimes A\underset{H}{\square} g} A \otimes A \underset{H}{\square} W \longrightarrow 0$$

é exata se, e somente se, a sequência:

$$0 \longrightarrow A \underset{H}{\square} U \xrightarrow{A\underset{H}{\square} f} A \underset{H}{\square} V \xrightarrow{A\underset{H}{\square} g} A \underset{H}{\square} W \longrightarrow 0$$

é exata.

Portanto, pelas três condições acima, A é fielmente H-coplano.

($\Leftarrow$) Provaremos apenas que se A é H-coplano, então A é $\mathbb{K}$-plano. Peter Schauenburg afirma em [3] que A fielmente H-coplano implica A fielmente $\mathbb{K}$-plano quando $A^{co\,H} \cong \mathbb{K}$.

Considere a seguinte sequência exata em $\mathcal{M}_{\mathbb{K}}$:

$$0 \longrightarrow U \xrightarrow{f} V \xrightarrow{g} W \longrightarrow 0$$

Temos que H é $\mathbb{K}$-plano. Logo, temos a seguinte sequência exata:

$$0 \longrightarrow H \otimes U \xrightarrow{H\otimes f} H \otimes V \xrightarrow{H\otimes g} H \otimes W \longrightarrow 0$$

Note que $H \otimes U$ é H-comódulo à esquerda com coação dada por $\Delta_H \otimes U$. Analogamente, temos que $H \otimes V$ e $H \otimes W$ são H-comódulos à esquerda. Como A é H-coplano, temos a seguinte sequência exata:

$$0 \longrightarrow A \underset{H}{\square} (H \otimes U) \xrightarrow{A\underset{H}{\square}(H\otimes f)} A \underset{H}{\square} (H \otimes V) \xrightarrow{A\underset{H}{\square}(H\otimes g)} A \underset{H}{\square} (H \otimes W) \longrightarrow 0$$

Pelo Lema 1.41, temos o seguinte diagrama comutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A\underset{H}{\square}(H\otimes U) & \xrightarrow{A\underset{H}{\square}(H\otimes f)} & A\underset{H}{\square}(H\otimes V) & \xrightarrow{A\underset{H}{\square}(H\otimes g)} & A\underset{H}{\square}(H\otimes W) & \longrightarrow & 0 \\ & & \cong\big\downarrow & & \big\downarrow\cong & & \big\downarrow\cong & & \\ 0 & \longrightarrow & (A\underset{H}{\square}H)\otimes U & \xrightarrow{(A\underset{H}{\square}H)\otimes f} & (A\underset{H}{\square}H)\otimes V & \xrightarrow{(A\underset{H}{\square}H)\otimes g} & (A\underset{H}{\square}H)\otimes W & \longrightarrow & 0 \end{array}$$

Mas pela Proposição 1.37, temos que $A \cong A\underset{H}{\square}H$. Logo a seguinte sequência é exata:

$$0 \longrightarrow A\otimes U \xrightarrow{A\otimes f} A\otimes V \xrightarrow{A\otimes g} A\otimes W \longrightarrow 0$$

Portanto A é $\mathbb{K}$-plano. $\square$

Teorema 1.77. *Seja H uma álgebra de Hopf. Então a Proposição 1.73 estabelece uma correspondência bijetora entre funtores monoidais exatos que comutam com somas diretas arbitrárias ${}^H\mathcal{M} \to \mathcal{M}_{\mathbb{K}}$ e objetos H-Galois fielmente $\mathbb{K}$-planos.*

Demonstração. Seja $\mathcal{F}\colon {}^H\mathcal{M} \to \mathcal{M}_{\mathbb{K}}$ um funtor monoidal exato que comuta com somas diretas arbitrárias. Pelo Teorema 1.43, existe um H-comódulo álgebra à direita A, que é H-coplano, tal que $\mathcal{F}(V) \cong A\underset{H}{\square}V$, $\forall V \in {}^H\mathcal{M}$. Como o funtor é monoidal, os morfismos ξ e ξ_0 são isomorfismos. Logo $\mathbb{K} \cong A\underset{H}{\square}\mathbb{K} \cong A^{co\,H}$.

Considere f o morfismo dado pela seguinte composição:

$$A\otimes A \xrightarrow{\rho_A\otimes\rho_A} A\underset{H}{\square}H \otimes A\underset{H}{\square}H \xrightarrow{\xi} A\underset{H}{\square}(H\otimes H) \xrightarrow{\cong} (A\underset{H}{\square}H)\otimes H \xrightarrow{\rho_A^{-1}\otimes H} A\otimes H$$

Como cada um dos morfismos é um isomorfismo, temos que f é isomorfismo. Aplicando em elementos, temos:

$$\begin{aligned} f(a\otimes b) &= (\rho_A^{-1}\otimes H)\circ\xi\circ(\rho_A\otimes\rho_A)(a\otimes b) \\ &= (\rho_A^{-1}\otimes H)\circ\xi\big(\sum a_{(0)}\otimes a_{(1)}\otimes b_{(0)}\otimes b_{(1)}\big) \\ &= (\rho_A^{-1}\otimes H)\big(\sum a_{(0)}b_{(0)}\otimes a_{(1)}\otimes b_{(1)}\big) \\ &= \sum \varepsilon(a_{(1)})a_{(0)}b_{(0)}\otimes b_{(1)} \\ &= \sum ab_{(0)}\otimes b_{(1)} \end{aligned}$$

Portanto f é a aplicação canônica de A e A é objeto H-Galois H-coplano. Pelo Lema 1.76, temos que A é objeto H-Galois fielmente $\mathbb{K}$-plano.

Reciprocamente, seja A um objeto H-Galois fielmente $\mathbb{K}$-plano. Temos que os morfismos:

$$\begin{aligned} \xi\colon (A\underset{H}{\square}V)\otimes(A\underset{H}{\square}W) &\longrightarrow A\underset{H}{\square}(V\otimes W) \\ (x\otimes v)\otimes(y\otimes w) &\longmapsto xy\otimes v\otimes w \end{aligned}$$

e

$$\begin{aligned} \xi_0\colon \mathbb{K} &\longrightarrow A\underset{H}{\square}\mathbb{K} \\ \alpha &\longmapsto 1\otimes\alpha \end{aligned}$$

definem uma estrutura de funtor monoidal fraco para $(A\underset{H}{\square}\_)\colon {}^H\mathcal{M} \to \mathcal{M}_{\mathbb{K}}$, que comuta com somas diretas arbitrárias. Como A é um objeto H-Galois, temos que $\mathbb{K} \cong A^{co\,H}$. Além disso, $A\underset{H}{\square}\mathbb{K} \cong A^{co\,H}$ e ξ_0 é monomorfismo, o que implica que ξ_0 é isomorfismo.

Considere o morfismo:

$$\begin{aligned} g\colon A\underset{H}{\square}(V\otimes W) &\longrightarrow (A\underset{H}{\square}V)\otimes(A\underset{H}{\square}W) \\ a\otimes v\otimes w &\longmapsto \sum a_{(0)}a_{(1)}^{[1]}\otimes v\otimes a_{(1)}^{[2]}\otimes w \end{aligned}$$

Então temos:

$$
\begin{aligned}
\xi \circ g(a \otimes v \otimes w) &= \xi(\sum a_{(0)} a_{(1)}^{[1]} \otimes v \otimes a_{(1)}^{[2]} \otimes w) \\
&= \sum a_{(0)} a_{(1)}^{[1]} a_{(1)}^{[2]} \otimes v \otimes w \\
&\overset{\text{Lema 1.75}}{=} a \otimes v \otimes w
\end{aligned}
$$

e

$$
\begin{aligned}
g \circ \xi(a \otimes v \otimes b \otimes w) &= g(ab \otimes v \otimes w) \\
&= \sum ab_{(0)} b_{(1)}^{[1]} \otimes v \otimes b_{(1)}^{[2]} \otimes w \\
&\overset{\text{Lema 1.75}}{=} a \otimes v \otimes b \otimes w
\end{aligned}
$$

Portanto g é a inversa de ξ, o que implica que ξ é isomorfismo e $(A \underset{H}{\square} \_)$ é funtor monoidal. Como A é fielmente $\mathbb{K}$-plano, pelo Lema 1.76, A é H-coplano e o funtor $(A \underset{H}{\square} \_)$ é exato. $\square$

Definição 1.78. *Sejam L e H álgebras de Hopf. Diremos que uma álgebra A é um objeto L-H-biGalois se: A é L-H-bicomódulo álgebra, é objeto L-Galois à esquerda e é objeto H-Galois à direita.*

Corolário 1.79. *Sejam H e R álgebras de Hopf, A um objeto H-Galois à direita e B um objeto H-R-biGalois fielmente $\mathbb{K}$-planos. Então $A \underset{H}{\square} B$ é um objeto R-Galois à direita fielmente $\mathbb{K}$-plano. Além disso, se L é uma álgebra de Hopf e A é um objeto L-H-biGalois fielmente $\mathbb{K}$-plano, então $A \underset{H}{\square} B$ é um objeto L-R-biGalois fielmente $\mathbb{K}$-plano.*

Demonstração. Pelo Teorema 1.77, os funtores $(A \underset{H}{\square} \_)$ e $(B \underset{R}{\square} \_)$ são monoidais, fielmente exatos e comutam com somas diretas arbitrárias. Logo, o funtor $((A \underset{H}{\square} B) \underset{R}{\square} \_) \cong (A \underset{H}{\square} (B \underset{R}{\square} \_))$ é monoidal, fielmente exato e comuta com somas diretas arbitrárias. Pelo Teorema 1.77, temos que $A \underset{H}{\square} B$ é um objeto R-Galois à direita fielmente $\mathbb{K}$-plano.

Pelo resultado análogo à esquerda, temos que $A \underset{H}{\square} B$ é um objeto L-Galois à esquerda fielmente $\mathbb{K}$-plano. Como a estrutura de L-comódulo à esquerda é dada por $\beta_A \otimes B$ e a estrutura de R-comódulo à direita é dada por $A \otimes \rho_B$, temos que $A \underset{H}{\square} B$ é um objeto L-R-biGalois. $\square$

O seguinte resultado é parte do Teorema 3.2.2 de [3] e não será demonstrado neste trabalho:

Proposição 1.80. *Para cada objeto L-H-biGalois $\mathbb{K}$-plano A, existe um objeto H-L-biGalois $\mathbb{K}$-plano A^{-1} tal que $A \underset{H}{\square} A^{-1} \cong L$ como L-L-bicomódulo álgebras e $A^{-1} \underset{L}{\square} A \cong H$ como H-H-bicomódulo álgebras.*

Definição 1.81. *Seja H uma álgebra de Hopf. Definimos:*

1) *Gal(H) como o conjunto das classes de equivalência por isomorfismo dos objetos H-Galois à direita fielmente $\mathbb{K}$-planos;*

2) *BiGal(H) como o conjunto das classes de equivalência por isomorfismo dos objetos H-biGalois fielmente $\mathbb{K}$-planos.*

Corolário 1.82. *O conjunto BiGal(H) é um grupo com o produto cotensorial.*

Demonstração. O Corolário 1.79 garante que o produto está bem definido.

Pelo Lema 1.41, temos que o produto é associativo.

Pela Proposição 1.37, temos que o elemento neutro é a álgebra de Hopf H.

Pela Proposição 1.80, temos a existência da inversa. Portanto BiGal(H) é um grupo com o produto cotensorial. $\square$

No Teorema 3.5 de [2], Schauenburg demonstra o seguinte resultado:

Teorema 1.83. *Sejam H uma álgebra de Hopf e A um objeto H-Galois à direita fielmente $\mathbb{K}$-plano. Então existe uma álgebra de Hopf $L := L(A, H)$ tal que A é um objeto L-H-biGalois. Seja β a estrutura de L-comódulo em A. Para qualquer biálgebra B e estrutura de B-comódulo β' em A que faz A ser um objeto B-H-biGalois, existe um único isomorfismo $f\colon L \to B$ de biálgebras tal que $\beta' = (f \otimes A) \circ \beta$.*

Proposição 1.84. *Sejam H_1 e H_2 duas álgebras de Hopf. Se existe um objeto H_1-H_2-biGalois fielmente $\mathbb{K}$-plano, então temos uma bijeção:*

$$Gal(H_1) \cong Gal(H_2)$$

e um isomorfismo de grupos:

$$BiGal(H_1) \cong BiGal(H_2)$$

Demonstração. Seja A um objeto H_1-H_2-biGalois fielmente $\mathbb{K}$-plano. Pela Proposição 1.80, existe um objeto H_2-H_1-biGalois A^{-1} tal que $A \underset{H_2}{\square} A^{-1} \cong H_1$ como H_1-H_1-bicomódulo álgebras e $A^{-1} \underset{H_1}{\square} A \cong H_2$ como H_2-H_2-bicomódulo álgebras.

Como A é fielmente $\mathbb{K}$-plano, pelo Lema 1.76, temos que o funtor $(A \underset{H_2}{\square} \_)$ é fielmente exato. Além disso, temos que $(A \underset{H_2}{\square} (A^{-1} \underset{H_1}{\square} \_)) \cong (H_1 \underset{H_1}{\square} \_)$ que, pela Proposição 1.37, é um funtor fielmente exato. Mas isto implica que o funtor $(A^{-1} \underset{H_1}{\square} \_)$ é fielmente exato. Pelo Lema 1.76, temos que A^{-1} é fielmente $\mathbb{K}$-plano.

Defina as seguintes funções:

$$\begin{aligned} \Psi\colon \mathrm{Gal}(H_1) &\longrightarrow \mathrm{Gal}(H_2) \\ B &\longmapsto B \underset{H_1}{\square} A \end{aligned}$$

e

$$\begin{aligned} \Phi\colon \mathrm{Gal}(H_2) &\longrightarrow \mathrm{Gal}(H_1) \\ C &\longmapsto C \underset{H_2}{\square} A^{-1} \end{aligned}$$

Temos que:

$$\begin{aligned} \Psi \circ \Phi(C) &= \Psi(C \underset{H_2}{\square} A^{-1}) \\ &= C \underset{H_2}{\square} A^{-1} \underset{H_1}{\square} A \\ &= C \underset{H_2}{\square} H_2 \\ &= C \end{aligned}$$

Analogamente, temos que $\Phi \circ \Psi(B) = B$. Portanto Ψ é uma bijeção com inversa dada por Φ.

Para os grupos $\mathrm{BiGal}(H_1)$ e $\mathrm{BiGal}(H_2)$, definimos:

$$\begin{aligned}\Psi'\colon \mathrm{BiGal}(H_1) &\longrightarrow \mathrm{BiGal}(H_2)\\ B &\longmapsto A^{-1} \underset{H_1}{\square} B \underset{H_1}{\square} A\end{aligned}$$

e

$$\begin{aligned}\Phi'\colon \mathrm{BiGal}(H_2) &\longrightarrow \mathrm{BiGal}(H_1)\\ C &\longmapsto A \underset{H_2}{\square} C \underset{H_2}{\square} A^{-1}\end{aligned}$$

Temos que:

$$\begin{aligned}\Psi'(B_1 \underset{H_1}{\square} B_2) &= A^{-1} \underset{H_1}{\square} B_1 \underset{H_1}{\square} B_2 \underset{H_1}{\square} A\\ &= A^{-1} \underset{H_1}{\square} B_1 \underset{H_1}{\square} H_1 \underset{H_1}{\square} B_2 \underset{H_1}{\square} A\\ &= A^{-1} \underset{H_1}{\square} B_1 \underset{H_1}{\square} A \underset{H_2}{\square} A^{-1} \underset{H_1}{\square} B_2 \underset{H_1}{\square} A\\ &= \Psi'(B_1) \underset{H_2}{\square} \Psi'(B_2)\end{aligned}$$

Portanto Ψ' é morfismo de grupos. Analogamente, temos que Φ' é morfismo de grupos. Além disso, temos que:

$$\begin{aligned}\Psi' \circ \Phi'(C) &= \Psi'(A \underset{H_2}{\square} C \underset{H_2}{\square} A^{-1})\\ &= A^{-1} \underset{H_1}{\square} A \underset{H_2}{\square} C \underset{H_2}{\square} A^{-1} \underset{H_1}{\square} A\\ &= H_2 \underset{H_2}{\square} C \underset{H_2}{\square} H_2\\ &= C\end{aligned}$$

Analogamente, temos que $\Phi' \circ \Psi'(B) = B$. Portanto Ψ' é um isomorfismo de grupos, com inversa dada por Φ'. $\square$

1.8 Produtos Cruzados

Nesta seção mostraremos a relação entre extensões fendidas e H-extensões Galois, com o objetivo de demonstrar o seguinte resultado: Sejam A_1 e A_2 H-extensões Galois de B e $T\colon A_1 \to A_2$ um morfismo de H-extensões Galois. Se A_1 é fendido, então A_2 é fendido e T é isomorfismo.

Definição 1.85. *Seja A uma H-extensão de B. Diremos que a extensão é fendida se existe um morfismo de H-comódulos $\gamma\colon H \to A$ invertível por convolução.*

Observação 1.86. *Note que podemos assumir que $\gamma(1) = 1$, pois caso $\gamma(1) \neq 1$, podemos trocar γ por $\gamma' = \gamma(1)^{-1}\gamma$, que também é invertível por convolução.*

Definição 1.87. *Sejam H uma álgebra de Hopf e A uma álgebra. Diremos que H mede A se existe um morfismo $\mathbb{K}$-linear, que denotaremos por:*

$$\begin{aligned}H \otimes A &\longrightarrow A\\ h \otimes a &\longmapsto h \cdot a\end{aligned}$$

tal que $\forall h \in H$ e $\forall a, b \in A$:

1) $h \cdot (ab) = \sum (h_1 \cdot a)(h_2 \cdot b)$

2) $h \cdot 1 = \varepsilon_H(h)1$

Definição 1.88. *Sejam H uma álgebra de Hopf e A uma álgebra. Diremos que A é um H-módulo álgebra se:*

1) H mede A;

2) tomando $\vartheta_A\colon H \otimes A \to A$ dado por $\vartheta_A(h \otimes a) = h \cdot a$, então (A, ϑ_A) é um H-módulo.

Neste caso, chamaremos ϑ_A de uma ação de H sobre A.

Definição 1.89. *Sejam H uma álgebra de Hopf, A uma álgebra e $\sigma\colon H \otimes H \to A$ um morfismo $\mathbb{K}$-linear invertível por convolução. Se H mede A, definimos o produto cruzado $A \underset{\sigma}{\#} H$ por:*

- *$A \underset{\sigma}{\#} H = A \otimes H$ como $\mathbb{K}$-módulos e denotamos por $a\#h$ o elemento $a \otimes h$ em $A \underset{\sigma}{\#} H$.*
- *A multiplicação em $A \underset{\sigma}{\#} H$ é dada por:*

$$(a\#h)(b\#k) = \sum a(h_1 \cdot b)\sigma h_2, k_1 \# h_3 k_2$$

Lema 1.90. *O produto cruzado $A \underset{\sigma}{\#} H$ é uma álgebra associativa com identidade $1\#1$ se, e somente se, valem as seguinte condições:*

1) Para todo $a \in A$ e $h, k \in H$ temos:

$$1 \cdot a = a$$

e

$$h \cdot (k \cdot a) = \sum \sigma(h_1, k_1)\big((h_2 k_2) \cdot a\big)\sigma^{-1}(h_3, k_3)$$

2) O morfismo σ é um cociclo de H, ou seja, para todo $h, k, l \in H$ temos:

$$\sigma(h, 1) = \varepsilon_H(h)1 = \sigma(1, h)$$

e

$$\sum (h_1 \cdot \sigma(k_1, l_1))\sigma(h_2, k_2 l_2) = \sum \sigma(h_1, k_1)\sigma(h_2 k_2, l)$$

Lema 1.91. *Seja A uma H-extensão fendida de B, com $\gamma\colon H \to A$ invertível por convolução e $\gamma(1) = 1$. Então H mede B com:*

$$h \cdot b = \sum \gamma(h_1) b \gamma^{-1}(h_2)$$

e temos que $\sigma\colon H \otimes H \to B$ dada por:

$$\sigma(h, k) = \sum \gamma(h_1)\gamma(k_1)\gamma^{-1}(h_2 k_2)$$

é invertível por convolução.

Além disso, $B \underset{\sigma}{\#} H \cong A$ como H-comódulo álgebras à direita e B-módulos à esquerda por:

$$\begin{aligned} \phi\colon B \underset{\sigma}{\#} H &\longrightarrow A \\ b\#h &\longmapsto b\gamma(h) \end{aligned}$$

Demonstração. Precisamos verificar que, se $b \in B = A^{co\,H}$, então $h \cdot b \in B$, ou seja, que $\rho_A(h \cdot b) = (h \cdot b) \otimes 1$. De fato, como γ é morfismo de H-comódulos, temos que:

$$\rho_A \circ \gamma = (\gamma \otimes H) \circ \Delta_H$$

Além disso, como ρ_A é morfismo de álgebras, temos que:

$$\rho \circ (\gamma^{-1}) = (\rho \circ \gamma)^{-1}$$

Além disso, tomando θ a função:

$$\begin{aligned} \theta \colon H &\longrightarrow A \otimes H \\ h &\longmapsto \gamma^{-1}(h_2) \otimes S(h_1) \end{aligned}$$

temos que:

$$\begin{aligned} ((\rho_A \circ \gamma) * \theta)(h) &= \sum (\gamma(h_1) \otimes h_2)(\gamma^{-1}(h_4) \otimes S(h_3)) \\ &= \sum \gamma(h_1)\gamma^{-1}(h_4) \otimes h_2 S(h_3) \\ &= \sum \gamma(h_1)\gamma^{-1}(h_3) \otimes \varepsilon_H(h_2)1 \\ &= \sum \gamma(\varepsilon_H(h_2)h_1)\gamma^{-1}(h_3) \otimes 1 \\ &= \sum \gamma(h_1)\gamma^{-1}(h_2) \otimes 1 \\ &= \varepsilon_H(h)(1 \otimes 1) \end{aligned}$$

ou seja, θ é a inversa por convolução pela direita de $\rho_A \circ \gamma$. Pela unicidade da inversa, temos que:

$$\rho \circ (\gamma^{-1}) = \theta$$

Logo:

$$\begin{aligned} \rho_A(h \cdot b) &= \rho_A\big(\sum \gamma(h_1) b \gamma^{-1}(h_2)\big) \\ &= \sum \rho_A(\gamma(h_1))\rho_A(b)\rho_A(\gamma^{-1}(h_2)) \\ &= \sum \rho_A(\gamma(h_1))\rho_A(b)\theta(h_2) \\ &= \sum (\gamma(h_1) \otimes h_2)(b \otimes 1)(\gamma^{-1}(h_4) \otimes S(h_3)) \\ &= \sum (\gamma(h_1) b \gamma^{-1}(h_4)) \otimes h_2 S(h_3) \\ &= \sum (\gamma(h_1) b \gamma^{-1}(h_3)) \otimes \varepsilon_H(h_2)1 \\ &= \sum (\gamma(\varepsilon_H(h_2)h_1) b \gamma^{-1}(h_3)) \otimes 1 \\ &= \sum (\gamma(h_1) b \gamma^{-1}(h_2)) \otimes 1 \\ &= (h \cdot b) \otimes 1 \end{aligned}$$

Portanto $h \cdot b \in A^{co\,H} = B$.

Veremos que as duas condições para H medir B são satisfeitas:

1) Para cada $h \in H$ e $a, b \in B$ temos:

$$\begin{aligned} h \cdot (ab) &= \sum \gamma(h_1) ab \gamma^{-1}(h_2) \\ &= \sum \gamma(h_1) ab \gamma^{-1}(\varepsilon_H(h_2)h_3) \\ &= \sum \gamma(h_1) a(\varepsilon_H(h_2)1) b \gamma^{-1}(h_3) \\ &= \sum \gamma(h_1) a(\gamma^{-1}(h_2)\gamma(h_3)) b \gamma^{-1}(h_4) \\ &= (h_1 \cdot a)(h_2 \cdot b) \end{aligned}$$

2) Para cada $h \in H$ temos:

$$\begin{aligned} h \cdot 1 &= \sum \gamma(h_1)1\gamma^{-1}(h_2) \\ &= (\gamma * \gamma^{-1})(h) \\ &= \varepsilon_H(h)1 \end{aligned}$$

Portanto H mede B com a estrutura dada.

Precisamos verificar que $\sigma(h,k) \in B$, $\forall h, k \in H$. De fato, temos:

$$\begin{aligned} \rho_A(\sigma(h,k)) &= \rho_A\big(\sum \gamma(h_1)\gamma(k_1)\gamma^{-1}(h_2k_2)\big) \\ &= \sum \rho_A(\gamma(h_1))\rho_A(\gamma(k_1))\rho_A(\gamma^{-1}(h_2k_2)) \\ &= \sum(\gamma(h_{1,1}) \otimes h_{1,2})(\gamma(k_{1,1}) \otimes k_{1,2})(\gamma^{-1}(h_{2,2}k_{2,2}) \otimes S(h_{2,1}k_{2,1})) \\ &= \sum(\gamma(h_{1,1})\gamma(k_{1,1})\gamma^{-1}(h_{2,2}k_{2,2})) \otimes h_{1,2}k_{1,2}S(h_{2,1}k_{2,1}) \\ &= \sum(\gamma(h_{1,1})\gamma(k_{1,1})\gamma^{-1}(h_{2,2}k_{2,2})) \otimes h_{1,2}k_{1,2}S(k_{2,1})S(h_{2,1}) \\ &= \sum(\gamma(h_1)\gamma(k_1)\gamma^{-1}(h_4k_4)) \otimes h_2k_2S(k_3)S(h_3) \\ &= \sum(\gamma(h_1)\gamma(k_1)\gamma^{-1}(h_3k_3)) \otimes \varepsilon_H(h_2)\varepsilon_H(k_2)1 \\ &= \sum(\gamma(\varepsilon_H(h_2)h_1)\gamma(\varepsilon_H(k_2)k_1)\gamma^{-1}(h_3k_3)) \otimes 1 \\ &= \sum(\gamma(h_1)\gamma(k_1)\gamma^{-1}(h_2k_2)) \otimes 1 \\ &= \sigma(h,k) \otimes 1 \end{aligned}$$

Portanto $\sigma(h,k) \in A^{co\,H} = B$.

Vejamos que σ é invertível por convolução. Tome $\tau(h,k) = \sum \gamma(h_1k_1)\gamma^{-1}(k_2)\gamma^{-1}(h_2)$. Então:

$$\begin{aligned} (\sigma * \tau)(h,k) &= \sum \sigma(h_1,k_1)\tau(h_2,k_2) \\ &= \sum \gamma(h_{1,1})\gamma(k_{1,1})\gamma^{-1}(h_{1,2}k_{1,2})\gamma(h_{2,1}k_{2,1})\gamma^{-1}(k_{2,2})\gamma^{-1}(h_{2,2}) \\ &= \sum \gamma(h_{1,1})\gamma(k_{1,1})\gamma^{-1}(h_{1,2}k_{1,2})\gamma(h_{2,1}k_{2,1})\gamma^{-1}(k_{2,2})\gamma^{-1}(h_{2,2}) \\ &= \sum \gamma(h_1)\gamma(k_1)\varepsilon_H(h_2k_2)\gamma^{-1}(k_3)\gamma^{-1}(h_3) \\ &= \sum \gamma(h_1)\gamma(k_1)\varepsilon_H(h_2)\varepsilon_H(k_2)\gamma^{-1}(k_3)\gamma^{-1}(h_3) \\ &= \sum \gamma(\varepsilon_H(h_2)h_1)\gamma(\varepsilon_H(k_2)k_1)\gamma^{-1}(k_3)\gamma^{-1}(h_3) \\ &= \sum \gamma(h_1)\gamma(k_1)\gamma^{-1}(k_2)\gamma^{-1}(h_2) \\ &= \varepsilon_H(k)\sum \gamma(h_1)\gamma^{-1}(h_2) \\ &= \varepsilon_H(h)\varepsilon_H(k)1 \end{aligned}$$

e

$$
\begin{aligned}
(\tau * \sigma)(h,k) &= \sum \tau(h_1,k_1)\sigma(h_2,k_2) \\
&= \sum \gamma(h_{1,1}k_{1,1})\gamma^{-1}(k_{1,2})\gamma^{-1}(h_{1,2})\gamma(h_{2,1})\gamma(k_{2,1})\gamma^{-1}(h_{2,2}k_{2,2}) \\
&= \sum \gamma(h_1k_1)\gamma^{-1}(k_2)\gamma^{-1}(h_{2,1})\gamma(h_{2,2})\gamma(k_3)\gamma^{-1}(h_3k_4) \\
&= \sum \gamma(h_1k_1)\gamma^{-1}(k_2)(\varepsilon_H(h_2)1)\gamma(k_3)\gamma^{-1}(h_3k_4) \\
&= \sum \gamma(\varepsilon_H(h_2)h_1k_1)\gamma^{-1}(k_{2,1})\gamma(k_{2,2})\gamma^{-1}(h_3k_3) \\
&= \sum \gamma(h_1k_1)(\varepsilon_H(k_2)1)\gamma^{-1}(h_2k_3) \\
&= \sum \gamma(\varepsilon_H(k_2)h_1k_1)\gamma^{-1}(h_2k_3) \\
&= \sum \gamma(h_1k_1)\gamma^{-1}(h_2k_2) \\
&= \varepsilon_H(hk)1 \\
&= \varepsilon_H(h)\varepsilon_H(k)1
\end{aligned}
$$

ou seja, τ é a inversa por convolução de σ.

Considere as funções:

$$
\begin{aligned}
\phi\colon B\underset{\sigma}{\#}H &\longrightarrow A \\
b\#h &\longmapsto b\gamma(h)
\end{aligned}
$$

e

$$
\begin{aligned}
\varphi\colon A &\longrightarrow B\underset{\sigma}{\#}H \\
a &\longmapsto \sum a_{(0)}\gamma^{-1}(a_{(1)})\#a_{(2)}
\end{aligned}
$$

Precisamos verificar que $\sum a_{(0)}\gamma^{-1}(a_{(1)}) \in B$. De fato:

$$
\begin{aligned}
\rho_A\left(\sum a_{(0)}\gamma^{-1}(a_{(1)})\right) &= \sum \rho_A(a_{(0)})\rho_A(\gamma^{-1}(a_{(1)})) \\
&= \sum (a_{(0,0)} \otimes a_{(0,1)})(\gamma^{-1}(a_{(1)2}) \otimes S(a_{(1)1})) \\
&= \sum a_{(0)}\gamma^{-1}(a_{(3)}) \otimes a_{(1)}S(a_{(2)}) \\
&= \sum a_{(0)}\gamma^{-1}(a_{(2)}) \otimes \varepsilon_H(a_{(1)})1 \\
&= \sum a_{(0)}\gamma^{-1}(\varepsilon_H(a_{(1)})a_{(2)}) \otimes 1 \\
&= \sum a_{(0)}\gamma^{-1}(a_{(1)}) \otimes 1
\end{aligned}
$$

Claramente ϕ é B-linear à esquerda. Vejamos que φ também é B-linear. De fato, se $b \in B$ e $a \in A$, então:

$$
\begin{aligned}
\varphi(ba) &= \sum (ba)_{(0)}\gamma^{-1}((ba)_{(1)})\#(ba)_{(2)} \\
&= \sum b_{(0)}a_{(0)}\gamma^{-1}(b_{(1)}a_{(1)})\#b_{(2)}a_{(2)} \\
&= \sum ba_{(0)}\gamma^{-1}(a_{(1)})\#a_{(2)} \\
&= b\varphi(a)
\end{aligned}
$$

Como $B\underset{\sigma}{\#}H$ é H-comódulo à direita com $\rho(b\#h) = \sum b\#h_1 \otimes h_2$, também é fácil verificar que as funções são morfismos de H-comódulos.

Vejamos que φ é a inversa de ϕ:

$$\begin{aligned}\phi\circ\varphi(a) &= \phi\big(\sum a_{(0)}\gamma^{-1}(a_{(1)})\#a_{(2)}\big)\\ &= \sum a_{(0)}\gamma^{-1}(a_{(1)})\gamma(a_{(2)})\\ &= \sum a_{(0)}\varepsilon_H(a_{(1)})\\ &= a\end{aligned}$$

e como $\rho_A\circ\gamma = (\gamma\otimes H)\circ\Delta_H$, temos que $(A\otimes\Delta_H)\circ\rho_A\circ\gamma = (\gamma\otimes\Delta_H)\circ\Delta_H$, ou seja:

$$\sum \gamma(h)_{(0)}\otimes\gamma(h)_{(1)}\otimes\gamma(h)_{(2)} = \sum \gamma(h_1)\otimes h_2\otimes h_3$$

Logo:

$$\begin{aligned}\varphi\circ\phi(b\#h) &= \varphi(b\gamma(h))\\ &= b\varphi(\gamma(h))\\ &= b\big(\sum \gamma(h)_{(0)}\gamma^{-1}(\gamma(h)_{(1)})\#\gamma(h)_{(2)}\big)\\ &= b\big(\sum \gamma(h_1)\gamma^{-1}(h_2)\#h_3\big)\\ &= b\big(\sum \varepsilon_H(h_1)1\#h_2\big)\\ &= b\big(\sum 1\#\varepsilon_H(h_1)h_2\big)\\ &= b\#h\end{aligned}$$

Portanto ϕ e φ são isomorfismos. □

Lema 1.92. *Seja* $A\underset{\sigma}{\#}H$ *um produto cruzado. Tomando:*

$$\begin{aligned}\gamma\colon H &\longrightarrow A\underset{\sigma}{\#}H\\ h &\longmapsto 1\#h\end{aligned}$$

então γ é morfismo de H-comódulos invertível por convolução, com inversa dada por:

$$\gamma^{-1}(h) = \sum \sigma^{-1}(S(h_2),h_3)\#S(h_1)$$

Em particular, $A\hookrightarrow A\underset{\sigma}{\#}H$ é uma H-extensão fendida.

Demonstração. Vejamos que γ é morfismo de H-comódulos. Precisamos que o seguinte diagrama comute:

$$\begin{array}{ccc} H & \xrightarrow{\quad\gamma\quad} & A\underset{\sigma}{\#}H \\ {\scriptstyle\rho_H}\downarrow & & \downarrow{\scriptstyle\rho_{A\underset{\sigma}{\#}H}} \\ H\otimes H & \xrightarrow{\ \gamma\otimes H\ } & A\underset{\sigma}{\#}H\otimes H \end{array}$$

De fato, para cada $h\in H$ temos:

$$\begin{aligned}\rho_{A\underset{\sigma}{\#}H}\circ\gamma(h) &= \rho_{A\underset{\sigma}{\#}H}(1\#h)\\ &= \sum 1\#h_1\otimes h_2\\ &= (\gamma\otimes H)(\sum h_1\otimes h_2)\\ &= (\gamma\otimes H)\circ\Delta_H(h)\\ &= (\gamma\otimes H)\circ\rho_H(h)\end{aligned}$$

Portanto γ é morfismo de H-comódulos.

Tomando $\mu\colon H \to A\underset{\sigma}{\#}H$ dado por $\mu(h) = \sum \sigma^{-1}(S(h_2), h_3)\#S(h_1)$, temos que para cada $h \in H$:

$$\begin{aligned}
(\mu * \gamma)(h) &= \sum \mu(h_1)\gamma(h_2)\\
&= \sum(\sigma^{-1}(S(h_{1,2}), h_{1,3})\#S(h_{1,1}))(1\#h_2)\\
&= \sum \sigma^{-1}(S(h_{1,2}), h_{1,3})(S(h_{1,1})_1 \cdot 1)\sigma(S(h_{1,1})_2, h_{2,1})\#S(h_{1,1})_3 h_{2,2}\\
&= \sum \sigma^{-1}(S(h_{1,2}), h_{1,3})(\varepsilon_H(S(h_{1,1})_1))\sigma(S(h_{1,1})_2, h_{2,1})\#S(h_{1,1})_3 h_{2,2}\\
&= \sum \sigma^{-1}(S(h_{1,2}), h_{1,3})\sigma(\varepsilon_H(S(h_{1,1})_1)S(h_{1,1})_2, h_{2,1})\#S(h_{1,1})_3 h_{2,2}\\
&= \sum \sigma^{-1}(S(h_{1,2}), h_{1,3})\sigma(S(h_{1,1})_1, h_{2,1})\#S(h_{1,1})_2 h_{2,2}\\
&= \sum \sigma^{-1}(S(h_{1,2}), h_{1,3})\sigma(S(h_{1,1,2}), h_{2,1})\#S(h_{1,1,1}) h_{2,2}\\
&= \sum \sigma^{-1}(S(h_3), h_4)\sigma(S(h_2), h_5)\#S(h_1)h_6\\
&= \sum \sigma^{-1}(S(h_{2,2}), h_{3,1})\sigma(S(h_{2,1}), h_{3,2})\#S(h_1)h_4\\
&= \sum \sigma^{-1}(S(h_2)_1, h_{3,1})\sigma(S(h_2)_2, h_{3,2})\#S(h_1)h_4\\
&= \sum(\sigma^{-1} * \sigma)(S(h_2), h_3)\#S(h_1)h_4\\
&= \sum \varepsilon_H(S(h_2))\varepsilon_H(h_3)\#S(h_1)h_4\\
&= \sum 1\#\varepsilon_H(S(h_1)_1)S(h_1)_2\varepsilon_H(h_2)h_3\\
&= \sum 1\#S(h_1)h_2\\
&= \varepsilon_H(h)1\#1
\end{aligned}$$

e

$$\begin{aligned}
(\gamma * \mu)(h) &= \sum \gamma(h_1)\mu(h_2)\\
&= \sum(1\#h_1)(\sigma^{-1}(S(h_{2,2}), h_{2,3})\#S(h_{2,1}))\\
&= \sum(h_{1,1} \cdot \sigma^{-1}(S(h_{2,2}), h_{2,3}))\sigma(h_{1,2}, S(h_{2,1})_1)\#h_{1,3}S(h_{2,1})_2\\
&= \sum(h_{1,1} \cdot \sigma^{-1}(S(h_{2,2}), h_{2,3}))\sigma(h_{1,2}, S(h_{2,1,2}))\#h_{1,3}S(h_{2,1,1})\\
&= \sum(h_{1,1} \cdot \sigma^{-1}(S(h_{2,2}), h_{2,3}))\sigma(h_{1,2}, S(h_{2,1}))\#h_{1,3,1}S(h_{1,3,2})\\
&= \sum(h_{1,1} \cdot \sigma^{-1}(S(h_{2,2}), h_{2,3}))\sigma(h_{1,2}, S(h_{2,1}))\#\varepsilon_H(h_{1,3})1\\
&= \sum(h_{1,1} \cdot \sigma^{-1}(S(h_{2,2}), h_{2,3}))\sigma(\varepsilon_H(h_{1,3})h_{1,2}, S(h_{2,1}))\#1\\
&= \sum(h_{1,1} \cdot \sigma^{-1}(S(h_{2,2}), h_{2,3}))\sigma(h_{1,2}, S(h_{2,1}))\#1\\
&= \sum(h_1 \cdot \sigma^{-1}(S(h_4), h_5))\sigma(h_2, S(h_3))\#1
\end{aligned}$$

Logo, precisamos apenas verificar que

$$\sum(h_1 \cdot \sigma^{-1}(S(h_4), h_5))\sigma(h_2, S(h_3)) = \varepsilon_H(h)1,\ \forall h \in H$$

Note que:

$$\begin{aligned}
\sum (h_1 \cdot \sigma(k_1,l_1))(h_2 \cdot \sigma^{-1}(k_2,l_2)) &= h \cdot \left(\sum \sigma(k_1,l_1)\sigma^{-1}(k_2,l_2)\right) \\
&= h \cdot ((\sigma * \sigma^{-1})(k,l)) \\
&= h \cdot (\varepsilon_H(k)\varepsilon_H(l)1) \\
&= \varepsilon_H(k)\varepsilon_H(l)(h \cdot 1) \\
&= \varepsilon_H(h)\varepsilon_H(k)\varepsilon_H(l)1
\end{aligned}$$

e

$$\begin{aligned}
\sum (h_1 \cdot \sigma^{-1}(k_1,l_1))(h_2 \cdot \sigma(k_2,l_2)) &= h \cdot \left(\sum \sigma^{-1}(k_1,l_1)\sigma(k_2,l_2)\right) \\
&= h \cdot ((\sigma^{-1} * \sigma)(k,l)) \\
&= h \cdot (\varepsilon_H(k)\varepsilon_H(l)1) \\
&= \varepsilon_H(k)\varepsilon_H(l)(h \cdot 1) \\
&= \varepsilon_H(h)\varepsilon_H(k)\varepsilon_H(l)1
\end{aligned}$$

ou seja, a função:

$$\begin{aligned}
H \otimes H \otimes H &\longrightarrow B \\
h \otimes k \otimes l &\longmapsto h \cdot \sigma^{-1}(k,l)
\end{aligned}$$

é a inversa por convolução da função:

$$\begin{aligned}
H \otimes H \otimes H &\longrightarrow B \\
h \otimes k \otimes l &\longmapsto h \cdot \sigma(k,l)
\end{aligned}$$

Por outro lado, temos que:

$$\sum (h_1 \cdot \sigma(k_1,l_1))\sigma(h_2,k_2l_2) = \sum \sigma(h_1,k_1)\sigma(h_2k_2,l)$$

o que implica que:

$$h \cdot \sigma(k,l) = \sum \sigma(h_1,k_1)\sigma(h_2k_2,l_1)\sigma^{-1}(h_3,k_3l_2)$$

e claramente a função:

$$\begin{aligned}
H \otimes H \otimes H &\longrightarrow B \\
h \otimes k \otimes l &\longmapsto \sum \sigma(h_1,k_1l_1)\sigma^{-1}(h_2k_2,l_2)\sigma^{-1}(h_3,k_3)
\end{aligned}$$

é a inversa por convolução da função:

$$\begin{aligned}
H \otimes H \otimes H &\longrightarrow B \\
h \otimes k \otimes l &\longmapsto \sum \sigma(h_1,k_1)\sigma(h_2k_2,l_1)\sigma^{-1}(h_3,k_3l_2)
\end{aligned}$$

Assim temos que:

$$h \cdot \sigma^{-1}(k,l) = \sum \sigma^{-1}(h_1,k_1l_1)\sigma^{-1}(h_2k_2,l_2)\sigma(h_3,k_3)$$

Logo:

$$
\begin{aligned}
&\sum(h_1\cdot\sigma^{-1}(S(h_4),h_5))\sigma(h_2,S(h_3))\\
&\qquad=\sum\sigma(h_{1,1},S(h_4)_1h_{5,1})\sigma^{-1}(h_{1,2}S(h_4)_2,h_{5,2})\sigma^{-1}(h_{1,3},S(h_4)_3)\sigma(h_2,S(h_3))\\
&\qquad=\sum\sigma(h_{1,1},S(h_{4,3})h_{5,1})\sigma^{-1}(h_{1,2}S(h_{4,2}),h_{5,2})\sigma^{-1}(h_{1,3},S(h_{4,1}))\sigma(h_2,S(h_3))\\
&\qquad=\sum\sigma(h_{1,1},S(h_{4,3})h_{5,1})\sigma^{-1}(h_{1,2}S(h_{4,2}),h_{5,2})\sigma^{-1}(h_{1,3},S(h_{4,1}))\sigma(h_2,S(h_3))\\
&\qquad=\sum\sigma(h_1,S(h_8)h_9)\sigma^{-1}(h_2S(h_7),h_{10})\sigma^{-1}(h_3,S(h_6))\sigma(h_4,S(h_5))\\
&\qquad=\sum\sigma(h_1,S(h_6)h_7)\sigma^{-1}(h_2S(h_5),h_8)\sigma^{-1}(h_{3,1},S(h_{4,2}))\sigma(h_{3,2},S(h_{4,1}))\\
&\qquad=\sum\sigma(h_1,S(h_6)h_7)\sigma^{-1}(h_2S(h_5),h_8)\sigma^{-1}(h_{3,1},S(h_4)_1)\sigma(h_{3,2},S(h_4)_2)\\
&\qquad=\sum\sigma(h_1,S(h_6)h_7)\sigma^{-1}(h_2S(h_5),h_8)\big(\varepsilon_H(h_3)\varepsilon_H(S(h_4))1\big)\\
&\qquad=\sum\sigma(h_1,S(h_6)h_7)\sigma^{-1}(\varepsilon_H(h_3)\varepsilon_H(S(h_4))h_2S(h_5),h_8)\\
&\qquad=\sum\sigma(h_1,S(h_4)h_5)\sigma^{-1}(h_2S(h_3),h_6)\\
&\qquad=\sum\sigma(h_1,\varepsilon_H(h_3)1)\sigma^{-1}(\varepsilon_H(h_2)1,h_4)\\
&\qquad=\sum\varepsilon_H(h_3)\varepsilon_H(h_2)\sigma(h_1,1)\sigma^{-1}(1,h_4)\\
&\qquad=\sum\sigma(\varepsilon_H(h_2)h_1,1)\sigma^{-1}(1,\varepsilon_H(h_3)h_4)\\
&\qquad=\sum\sigma(h_1,1)\sigma^{-1}(1,h_2)\\
&\qquad=\sum\varepsilon_H(h_1)\varepsilon_H(h_2)1\\
&\qquad=\varepsilon_H(h)1
\end{aligned}
$$

Portanto γ é invertível por convolução com inversa dada por:

$$\gamma^{-1}(h)=\sum\sigma^{-1}(S(h_2),h_3)\#S(h_1)$$

$\square$

A partir dos dois últimos resultados, temos a seguinte proposição.

Proposição 1.93. *Seja A uma H-extensão Galois de B. Então a extensão é fendida se, e somente se, $A=B\underset{\sigma}{\#}H$.*

Agora apresentamos o resultado principal desta seção.

Teorema 1.94. *[5, Lema 8.5] Sejam A_1 e A_2 H-extensões Galois de B e $T\colon A_1\to A_2$ um morfismo de H-extensões. Se A_1 é fendido, então A_2 é fendido e T é isomorfismo.*

Demonstração. Seja $\gamma\colon H\to A_1$ um morfismo de H-comódulos invertível por convolução.

Pela Lema 1.91, temos que H mede B com:

$$h\underset{\gamma}{\cdot}b=\sum\gamma(h_1)b\gamma^{-1}(h_2)$$

temos que $\sigma_\gamma\colon H\otimes H\to B$ dada por:

$$\sigma_\gamma(h,k)=\sum\gamma(h_1)\gamma(k_1)\gamma^{-1}(h_2k_2)$$

é invertível por convolução e a função:

$$\begin{aligned} \phi_1 \colon B \underset{\sigma_\gamma}{\#} H &\longrightarrow A_1 \\ b\#h &\longmapsto b\gamma(h) \end{aligned}$$

é isomorfismo.

Como γ e T são morfismos de H-comódulos, temos que o seguinte diagrama comuta:

$$\begin{tikzcd} H \arrow[r, "\gamma"] \arrow[d, "\Delta_H"'] & A_1 \arrow[r, "T"] \arrow[d, "\rho_{A_1}"] & A_2 \arrow[d, "\rho_{A_2}"] \\ H \otimes H \arrow[r, "\gamma\otimes H"'] & A_1 \otimes H \arrow[r, "T\otimes H"'] & A_2 \otimes H \end{tikzcd}$$

Logo $T \circ \gamma \colon H \to A_2$ é morfismo de H-comódulos. Como T é morfismo de álgebras, temos que:

$$\begin{aligned} ((T \circ \gamma) * (T \circ \gamma^{-1})) &= T(\gamma * \gamma^{-1}) \\ &= T(u_{A_1}\varepsilon_H) \\ &= u_{A_2}\varepsilon_H \end{aligned}$$

ou seja, $T \circ \gamma^{-1}$ é a inversa por convolução à direita de $T \circ \gamma$. De forma análoga temos que $T \circ \gamma^{-1}$ é a inversa por convolução à esquerda de $T \circ \gamma$.

Portanto $T \circ \gamma$ é invertível por convolução e A_2 é fendido.

Pela Lema 1.91, temos que H mede B com:

$$h \underset{T\gamma}{\cdot} b = \sum (T \circ \gamma)(h_1) b (T \circ \gamma)^{-1}(h_2)$$

temos que $\sigma_{T\gamma} \colon H \otimes H \to B$ dada por:

$$\sigma_{T\gamma}(h,k) = \sum (T \circ \gamma(h_1))(T \circ \gamma)(k_1)(T \circ \gamma)^{-1}(h_2 k_2)$$

é invertível por convolução e a função:

$$\begin{aligned} \phi_2 \colon B \underset{\sigma_{T\gamma}}{\#} H &\longrightarrow A_2 \\ b\#h &\longmapsto b(T \circ \gamma)(h) \end{aligned}$$

é isomorfismo.

Como $T(b) = b$, $\forall b \in B$, $(T \circ \gamma)^{-1} = T \circ \gamma^{-1}$ e $h \underset{\gamma}{\cdot} b \in B$, temos que, $\forall h \in H$ e $b \in B$:

$$\begin{aligned} h \underset{T\gamma}{\cdot} b &= \sum (T \circ \gamma)(h_1) b (T \circ \gamma)^{-1}(h_2) \\ &= \sum (T \circ \gamma)(h_1) T(b) (T \circ \gamma^{-1})(h_2) \\ &= T\big(\sum \gamma(h_1) b \gamma^{-1}(h_2)\big) \\ &= T(h \underset{\gamma}{\cdot} b) \\ &= h \underset{\gamma}{\cdot} b \end{aligned}$$

e como $\sigma_\gamma(h,k) \in B$, temos que, $\forall h, k \in H$:

$$\begin{aligned} \sigma_{T\gamma}(h,k) &= \sum (T \circ \gamma(h_1))(T \circ \gamma)(k_1)(T \circ \gamma)^{-1}(h_2 k_2) \\ &= \sum (T \circ \gamma(h_1))(T \circ \gamma)(k_1)(T \circ \gamma^{-1})(h_2 k_2) \\ &= T\big(\sum \gamma(h_1)\gamma(k_1)\gamma^{-1}(h_2 k_2)\big) \\ &= T(\sigma_\gamma(h,k)) \\ &= \sigma_\gamma(h,k) \end{aligned}$$

Portanto $B\underset{\sigma_\gamma}{\#}H = B\underset{\sigma_{T\gamma}}{\#}H$. Além disso, temos:

$$\begin{aligned} T\circ\phi_1(b\#h) &= T(b\gamma(h)) \\ &= T(b)T(\gamma(h)) \\ &= b(T\circ\gamma)(h) \\ &= \phi_2(b\#h) \end{aligned}$$

ou seja, o seguinte diagrama comuta:

$$\begin{tikzcd} A_1 \arrow[rr, "T"] & & A_2 \\ & B\underset{\sigma_\gamma}{\#}H \arrow[ul, "\phi_1"] \arrow[ur, "\phi_2"'] & \end{tikzcd}$$

Como ϕ_1 e ϕ_2 são isomorfismos, temos que T é isomorfismo. □

Observação 1.95. *Sejam H uma álgebra de Hopf e $\sigma\colon H\otimes H\to\mathbb{K}$ um morfismo $\mathbb{K}$-linear invertível por convolução. Denotaremos o produto cruzado $\mathbb{K}\underset{\sigma}{\#}H$ por ${}_\sigma H$.*

Teorema 1.96. *[9, Proposição 2.4] Seja H uma álgebra de Hopf. Então se H tem dimensão finita, todo objeto H-Galois é fendido.*

Este teorema é essencial para o estudo dos objetos H-Galois que será feito nos Capítulos 2 e 3.

1.9 Cohomologia de Grupos

Nesta seção apresentaremos os grupos $Z^2(G,\mathbb{K}^*)$ e $B^2(G,\mathbb{K}^*)$, a fim de utilizarmos o quociente $H^2(G,\mathbb{K}^*) = Z^2(G,\mathbb{K}^*)/B^2(G,\mathbb{K}^*)$, com a notação apresentada por Gregory Karpilovsky em [8].

Definição 1.97. *Seja G um grupo. Definimos $Z^2(G,\mathbb{K}^*)$ como o grupo:*

$$Z^2(G,\mathbb{K}^*) = \{\sigma\colon G\times G\to\mathbb{K}^*;\ \sigma(h,1)=1=\sigma(1,h)\ \textit{e}\ \sigma(h,k)\sigma(hk,l)=\sigma(h,kl)\sigma(k,l)\}$$

Um elemento $\sigma\in Z^2(G,\mathbb{K}^*)$ será chamado de um cociclo de G.

Definição 1.98. *Seja G um grupo. Definimos a função bordo como:*

$$\begin{aligned} \partial\colon \mathit{Hom}(G,\mathbb{K}^*) &\longrightarrow \mathit{Hom}(G\times G,\mathbb{K}^*) \\ f &\longmapsto (g\times h\mapsto f(g)f(h)f(gh)^{-1}) \end{aligned}$$

e tomamos $B^2(G,\mathbb{K}^*)$ como o grupo:

$$B^2(G,\mathbb{K}^*) = \{\partial(f);\ f\colon G\to\mathbb{K}^*\ \textit{tal que}\ f(1)=1\}$$

Proposição 1.99. *Seja G um grupo. Então $B^2(G,\mathbb{K}^*)\subset Z^2(G,\mathbb{K}^*)$.*

Demonstração. Seja $f\colon G\to\mathbb{K}^*$ tal que $f(1)=1$. Então para cada $h,h,l\in G$ temos:

$$\begin{aligned} \partial(f)(h,k)\partial(f)(hk,l) &= f(h)f(k)f(hk)^{-1}f(hk)f(l)f(hkl)^{-1} \\ &= f(h)f(k)f(l)f(hkl)^{-1} \\ &= f(k)f(l)f(kl)^{-1}f(h)f(kl)f(hkl)^{-1} \\ &= \partial(f)(k,l)\partial(f)(h,kl) \end{aligned}$$

e

$$\begin{aligned}\partial(f)(h,1) &= f(h)f(1)f(h1)^{-1}\\ &= f(h)f(h)^{-1}\\ &= 1\\ &= f(h)f(h)^{-1}\\ &= f(1)f(h)f(1h)^{-1}\\ &= \partial(f)(1,h)\end{aligned}$$

Portanto $\partial(f) \in Z^2(G, \mathbb{K}^*)$. □

Definição 1.100. *Seja G um grupo. Definimos $H^2(G, \mathbb{K}^*)$ como:*

$$H^2(G, \mathbb{K}^*) = Z^2(G, \mathbb{K}^*)/B^2(G, \mathbb{K}^*)$$

Proposição 1.101. *Seja G um grupo e $\sigma\colon \mathbb{K}G \otimes \mathbb{K}G \to \mathbb{K}$ um cociclo tal que ${}_\sigma\mathbb{K}G$ é uma álgebra associativa. Então σ restrito à $G \times G$ pertence à $Z^2(G, \mathbb{K}^*)$.*

Demonstração. Segue direto do Lema 1.90, pois em $\mathbb{K}G$ temos $\Delta(h) = h \otimes h$ e $\varepsilon(h) = 1$, $\forall h \in G$. □

Proposição 1.102. *Seja G um grupo e $\sigma, \sigma'\colon \mathbb{K}G \otimes \mathbb{K}G \to \mathbb{K}$ cociclos tais que ${}_\sigma\mathbb{K}G$ e ${}_{\sigma'}\mathbb{K}G$ são álgebras associativas. Então ${}_\sigma\mathbb{K}G \cong {}_{\sigma'}\mathbb{K}G$ como $\mathbb{K}G$-comódulo álgebras à direita se, e somente se, $\sigma\sigma'^{-1}$ restrito à $G \times G$ pertence à $B^2(G, \mathbb{K}^*)$.*

Demonstração. ($\Rightarrow$) Sejam ρ e ρ' as estruturas de $\mathbb{K}G$-comódulo de ${}_\sigma\mathbb{K}G$ e ${}_{\sigma'}\mathbb{K}G$ respectivamente e seja $f\colon {}_\sigma\mathbb{K}G \to {}_{\sigma'}\mathbb{K}G$ um isomorfismo de $\mathbb{K}G$-comódulo álgebras à direita. Então:

$$\rho' \circ f = (f \otimes \mathbb{K}G) \circ \rho$$

Para cada $h \in G$, temos:

$$\begin{aligned}\rho' \circ f(h) &= \rho'\big(\sum_{g\in G} \alpha_g g\big)\\ &= \sum_{g\in G} \alpha_g g \otimes g\end{aligned}$$

e

$$\begin{aligned}(f \otimes \mathbb{K}G) \circ \rho(h) &= (f \otimes \mathbb{K}G)(h \otimes h)\\ &= f(h) \otimes h\end{aligned}$$

Daí temos que $\alpha_g = 0$ se $g \neq h$. Logo $f(h) = \alpha_h h$, $\forall h \in G$.
Defina a função:

$$\begin{aligned}u\colon G &\longrightarrow \mathbb{K}*\\ h &\longmapsto \alpha_h\end{aligned}$$

Como f é morfismo de álgebras, temos que:

$$f(h \underset{\sigma}{\cdot} g) = f(h) \underset{\sigma'}{\cdot} f(g)$$

Por um lado, temos:

$$\begin{aligned}f(h \underset{\sigma}{\cdot} g) &= f(\sigma(h,g)hg)\\ &= \sigma(h,g)u(hg)hg\end{aligned}$$

Por outro lado, temos:

$$\begin{aligned} f(h) \underset{\sigma'}{\cdot} f(g) &= (u(h)h) \underset{\sigma'}{\cdot} (u(g)g) \\ &= u(h)u(g)h \underset{\sigma'}{\cdot} g \\ &= u(h)u(g)\sigma'(h,g)hg \end{aligned}$$

Como $hg \neq 0$, temos:

$$\sigma(h,g)u(hg) = u(h)u(g)\sigma'(h,g)$$

ou seja:

$$\sigma(h,g)\sigma'(h,g)^{-1} = u(h)u(g)u(hg)^{-1} = \partial(u)(h,g)$$

Portanto $\sigma\sigma'^{-1}$ restrito à $G \times G$ pertence à $B^2(G, \mathbb{K}^*)$.
($\Leftarrow$) Como $\sigma\sigma'^{-1} \in B^2(G, \mathbb{K}^*)$, existe $u\colon G \to \mathbb{K}^*$ tal que $\sigma\sigma'^{-1} = \partial(u)$. Defina a função:

$$\begin{aligned} f\colon {}_{\sigma}\mathbb{K}G &\longrightarrow {}_{\sigma'}\mathbb{K}G \\ h &\longmapsto u(h)h \end{aligned}$$

Claramente f é isomorfismo, pois possui inversa dada por:

$$\begin{aligned} f^{-1}\colon {}_{\sigma'}\mathbb{K}G &\longrightarrow {}_{\sigma}\mathbb{K}G \\ h &\longmapsto u(h)^{-1}h \end{aligned}$$

Vejamos que f é um morfismo de $\mathbb{K}G$-comódulos à direita. Para cada $h \in G$ temos:

$$\begin{aligned} \rho' \circ f(h) &= \rho'(u(h)h) \\ &= u(h)(h \otimes h) \end{aligned}$$

e

$$\begin{aligned} (f \otimes \mathbb{K}G) \circ \rho(h) &= (f \otimes \mathbb{K}G)(h \otimes h) \\ &= f(h) \otimes h \\ &= u(h)h \otimes h \end{aligned}$$

Portanto f é morfismo de $\mathbb{K}G$-comódulos.
Vejamos que f é morfismo de álgebras. Para cada $h, g \in G$, temos:

$$\begin{aligned} f(h \underset{\sigma}{\cdot} g) &= f(\sigma(h,g)hg) \\ &= \sigma(h,g)u(hg)hg \end{aligned}$$

e

$$\begin{aligned} f(h) \underset{\sigma'}{\cdot} f(g) &= (u(h)h) \underset{\sigma'}{\cdot} (u(g)g) \\ &= u(h)u(g)(h \underset{\sigma'}{\cdot} g) \\ &= u(h)u(g)\sigma'(h,g)hg \end{aligned}$$

Como $\sigma(h,g)u(hg) = u(h)u(g)\sigma'(h,g)$, temos que f é morfismo de álgebras.
Portanto ${}_{\sigma}\mathbb{K}G$ e ${}_{\sigma'}\mathbb{K}G$ são isomorfos como $\mathbb{K}G$-comódulo álgebras. $\square$

2. DESCRIÇÃO DOS OBJETOS $A(\mathbb{G})$-GALOIS

2.1 A álgebra de Hopf $A(\mathbb{G})$

Nesta seção descreveremos a álgebra de Hopf $A(\mathbb{G})$, o principal objeto de estudo deste trabalho. Chen, Huang, Ye e Zhang mostram, em [7], que toda álgebra de Hopf monomial não semi-simples tem esta forma.

Definição 2.1. *Um conjunto de dados de grupo é uma quádrupla $\mathbb{G} = (G, g, \chi, \mu)$, onde G é um grupo finito, $g \in G$ é um elemento central, $\chi\colon G \to \mathbb{K}^*$ é um morfismo de grupos com $\chi(g) \neq 1$ e um elemento $\mu \in \mathbb{K}$ tal que se $o(\chi(g)) = o(g)$, então $\mu = 0$ e se $\mu \neq 0$, então $\chi^{o(\chi(g))} = 1$.*

Denotaremos por d a ordem de $\chi(g)$, ou seja $d = o(\chi(g))$. Quando $\mu = 0$, escrevemos apenas $\mathbb{G} = (G, g, \chi)$.

Definição 2.2. *Sejam $\mathbb{G} = (G, g, \chi, \mu)$ e $\mathbb{G}' = (G', g', \chi', \mu')$ dois conjuntos de dados de grupo. Dizemos que $\mathbb{G}$ é isomorfo a $\mathbb{G}'$ se existe uma constante $\eta \neq 0$ tal que $\mu = \eta^d \mu'$ e existe um isomorfismo $u\colon G \to G'$ tal que $u(g) = g'$ e $\chi' \circ u = \chi$.*

Definição 2.3. *Sejam $\mathcal{V}_0(\mathbb{G})$ o $\mathbb{K}$-módulo com base B,onde $B = \{y\} \bigcup \{w_h;\, h \in G\}$ e $\mathcal{L}_0(\mathbb{G})$ a álgebra tensorial sobre $\mathcal{V}_0(\mathbb{G})$. Definimos $\mathcal{I}_0(\mathbb{G})$ como o ideal bilateral de $\mathcal{L}_0(\mathbb{G})$ gerado por:*

$$\begin{gathered} w_{h_1} w_{h_2} - w_{h_1 h_2} \\ w_1 - 1 \\ y w_h - \chi(h) w_h y \\ y^d - \mu\,(1 - w_{g^d}) \end{gathered}$$

Chamaremos de $A(\mathbb{G})$ a álgebra quociente $\mathcal{L}_0(\mathbb{G})/\mathcal{I}_0(\mathbb{G})$. Note que o produto das classes de w_h em $A(\mathbb{G})$ é compatível com o produto do grupo G. Denotaremos a classe lateral de y por x e a classe lateral de w_h por h em $A(\mathbb{G})$, $\forall h \in G$.

Proposição 2.4. *O $\mathbb{K}$-módulo $\mathcal{V}_0(\mathbb{G})$ é uma coálgebra com:*

$$\begin{aligned} \Delta_{\mathcal{V}_0(\mathbb{G})}\colon \mathcal{V}_0(\mathbb{G}) &\longrightarrow \mathcal{V}_0(\mathbb{G}) \otimes \mathcal{V}_0(\mathbb{G}) \\ y &\longmapsto 1 \otimes y + y \otimes w_g \\ w_h &\longmapsto w_h \otimes w_h \end{aligned}$$

$$\begin{aligned} \varepsilon_{\mathcal{V}_0(\mathbb{G})}\colon \mathcal{V}_0(\mathbb{G}) &\longrightarrow \mathbb{K} \\ y &\longmapsto 0 \\ w_h &\longmapsto 1 \end{aligned}$$

Demonstração. Vejamos que os seguintes diagramas comutam:

$$\begin{tikzcd} \mathcal{V}_0(\mathbb{G}) \arrow[r, "\Delta_{\mathcal{V}_0(\mathbb{G})}"] \arrow[d, "\Delta_{\mathcal{V}_0(\mathbb{G})}"'] & \mathcal{V}_0(\mathbb{G}) \otimes \mathcal{V}_0(\mathbb{G}) \arrow[d, "\mathcal{V}_0(\mathbb{G}) \otimes \Delta_{\mathcal{V}_0(\mathbb{G})}"] \\ \mathcal{V}_0(\mathbb{G}) \otimes \mathcal{V}_0(\mathbb{G}) \arrow[r, "\Delta_{\mathcal{V}_0(\mathbb{G})} \otimes \mathcal{V}_0(\mathbb{G})"] & \mathcal{V}_0(\mathbb{G}) \otimes \mathcal{V}_0(\mathbb{G}) \otimes \mathcal{V}_0(\mathbb{G}) \end{tikzcd}$$

$$\begin{tikzcd}
 & \mathcal{V}_0(\mathbb{G}) \arrow[dl, "\cong"'] \arrow[dd, "\Delta_{\mathcal{V}_0(\mathbb{G})}"] \arrow[dr, "\cong"] & \\
\mathbb{K}\otimes\mathcal{V}_0(\mathbb{G}) & & \mathcal{V}_0(\mathbb{G})\otimes\mathbb{K} \\
 & \mathcal{V}_0(\mathbb{G})\otimes\mathcal{V}_0(\mathbb{G}) \arrow[ul, "\varepsilon_{\mathcal{V}_0(\mathbb{G})}\otimes\mathcal{V}_0(\mathbb{G})"] \arrow[ur, "\mathcal{V}_0(\mathbb{G})\otimes\varepsilon_{\mathcal{V}_0(\mathbb{G})}"'] &
\end{tikzcd}$$

De fato:

$$\begin{aligned}
(\Delta_{\mathcal{V}_0(\mathbb{G})}\otimes\mathcal{V}_0(\mathbb{G}))\circ\Delta_{\mathcal{V}_0(\mathbb{G})}(y) &= (\Delta_{\mathcal{V}_0(\mathbb{G})}\otimes\mathcal{V}_0(\mathbb{G}))(1\otimes y+y\otimes w_g)\\
&= 1\otimes 1\otimes y+(1\otimes y+y\otimes w_g)\otimes w_g\\
&= 1\otimes 1\otimes y+1\otimes y\otimes w_g+y\otimes w_g\otimes w_g\\
&= 1\otimes(1\otimes y+y\otimes w_g)+y\otimes w_g\otimes w_g\\
&= (\mathcal{V}_0(\mathbb{G})\otimes\Delta_{\mathcal{V}_0(\mathbb{G})})(1\otimes y+y\otimes w_g)\\
&= (\mathcal{V}_0(\mathbb{G})\otimes\Delta_{\mathcal{V}_0(\mathbb{G})})\circ\Delta_{\mathcal{V}_0(\mathbb{G})}(y)
\end{aligned}$$

e para cada $h\in G$:

$$\begin{aligned}
(\Delta_{\mathcal{V}_0(\mathbb{G})}\otimes\mathcal{V}_0(\mathbb{G}))\circ\Delta_{\mathcal{V}_0(\mathbb{G})}(w_h) &= (\Delta_{\mathcal{V}_0(\mathbb{G})}\otimes\mathcal{V}_0(\mathbb{G}))(w_h\otimes w_h)\\
&= w_h\otimes w_h\otimes w_h\\
&= (\mathcal{V}_0(\mathbb{G})\otimes\Delta_{\mathcal{V}_0(\mathbb{G})})(w_h\otimes w_h)\\
&= (\mathcal{V}_0(\mathbb{G})\otimes\Delta_{\mathcal{V}_0(\mathbb{G})})\circ\Delta_{\mathcal{V}_0(\mathbb{G})}(w_h)
\end{aligned}$$

Além disso, temos:

$$\begin{aligned}
(\mathcal{V}_0(\mathbb{G})\otimes\varepsilon_{\mathcal{V}_0(\mathbb{G})})\circ\Delta_{\mathcal{V}_0(\mathbb{G})}(y) &= (\mathcal{V}_0(\mathbb{G})\otimes\varepsilon_{\mathcal{V}_0(\mathbb{G})})(1\otimes y+y\otimes w_g)\\
&= y\otimes 1\\
&= \tau_{\mathcal{V}_0(\mathbb{G})}(y)
\end{aligned}$$

e para cada $h\in G$:

$$\begin{aligned}
(\mathcal{V}_0(\mathbb{G})\otimes\varepsilon_{\mathcal{V}_0(\mathbb{G})})\circ\Delta_{\mathcal{V}_0(\mathbb{G})}(w_h) &= (\mathcal{V}_0(\mathbb{G})\otimes\varepsilon_{\mathcal{V}_0(\mathbb{G})})(w_h\otimes w_h)\\
&= w_h\otimes 1\\
&= \tau_{\mathcal{V}_0(\mathbb{G})}(w_h)
\end{aligned}$$

À esquerda temos um resultado análogo. Portanto $\mathcal{V}_0(\mathbb{G})$ é coálgebra. $\square$

Pela Proposição 1.46, temos o seguinte resultado: A álgebra $\mathcal{L}_0(\mathbb{G})$ é biálgebra com:

$$\begin{aligned}
\Delta_{\mathcal{L}_0(\mathbb{G})}\colon \mathcal{L}_0(\mathbb{G}) &\longrightarrow \mathcal{L}_0(\mathbb{G})\otimes\mathcal{L}_0(\mathbb{G})\\
y &\longmapsto 1\otimes y+y\otimes w_g\\
w_h &\longmapsto w_h\otimes w_h
\end{aligned}$$

$$\begin{aligned}
\varepsilon_{\mathcal{L}_0(\mathbb{G})}\colon \mathcal{L}_0(\mathbb{G}) &\longrightarrow \mathbb{K}\\
y &\longmapsto 0\\
w_h &\longmapsto 1
\end{aligned}$$

Proposição 2.5. *A álgebra $A(\mathbb{G})$ é uma biálgebra com:*

$$\begin{aligned}\Delta_{A(\mathbb{G})} \colon A(\mathbb{G}) &\longrightarrow A(\mathbb{G}) \otimes A(\mathbb{G})\\ x &\longmapsto 1 \otimes x + x \otimes g\\ h &\longmapsto h \otimes h\end{aligned}$$

$$\begin{aligned}\varepsilon_{A(\mathbb{G})} \colon A(\mathbb{G}) &\longrightarrow \mathbb{K}\\ x &\longmapsto 0\\ h &\longmapsto 1\end{aligned}$$

e $\{hx^i;\, h \in G, 0 \leq i \leq d-1\}$ é base de $A(\mathbb{G})$ como $\mathbb{K}$-espaço vetorial.

Demonstração. Temos que $\mathcal{I}_0(\mathbb{G})$ é um ideal de $\mathcal{L}_0(\mathbb{G})$. Logo $A(\mathbb{G})$ é álgebra e a projeção:

$$\pi_{\mathcal{I}_0(\mathbb{G})} \colon \mathcal{L}_0(\mathbb{G}) \longrightarrow A(\mathbb{G})$$

é morfismo de álgebras. Vejamos que $\mathcal{I}_0(\mathbb{G})$ é um coideal. Utilizaremos o seguinte fato: Como $\ker \pi_{\mathcal{I}_0(\mathbb{G})} = \mathcal{I}_0(\mathbb{G})$, então $\ker\left(\pi_{\mathcal{I}_0(\mathbb{G})} \otimes \pi_{\mathcal{I}_0(\mathbb{G})}\right) = \mathcal{I}_0(\mathbb{G}) \otimes \mathcal{L}_0(\mathbb{G}) + \mathcal{L}_0(\mathbb{G}) \otimes \mathcal{I}_0(\mathbb{G})$. Nos geradores de $\mathcal{I}_0(\mathbb{G})$, temos:

$$\begin{aligned}&(\pi_{\mathcal{I}_0(\mathbb{G})} \otimes \pi_{\mathcal{I}_0(\mathbb{G})}) \circ \Delta_{\mathcal{L}(\mathbb{G})}(w_{h_1}w_{h_2} - w_{h_1h_2})\\ &\qquad= (\pi_{\mathcal{I}_0(\mathbb{G})} \otimes \pi_{\mathcal{I}_0(\mathbb{G})})\big((w_{h_1} \otimes w_{h_1})(w_{h_2} \otimes w_{h_2}) - w_{h_1h_2} \otimes w_{h_1h_2}\big)\\ &\qquad= (\pi_{\mathcal{I}_0(\mathbb{G})} \otimes \pi_{\mathcal{I}_0(\mathbb{G})})\big(w_{h_1}w_{h_2} \otimes w_{h_1}w_{h_2} - w_{h_1h_2} \otimes w_{h_1h_2}\big)\\ &\qquad= h_1h_2 \otimes h_1h_2 - h_1h_2 \otimes h_1h_2\\ &\qquad= 0\end{aligned}$$

$$\begin{aligned}&(\pi_{\mathcal{I}_0(\mathbb{G})} \otimes \pi_{\mathcal{I}_0(\mathbb{G})}) \circ \Delta_{\mathcal{L}(\mathbb{G})}(w_1 - 1)\\ &\qquad= (\pi_{\mathcal{I}_0(\mathbb{G})} \otimes \pi_{\mathcal{I}_0(\mathbb{G})})(w_1 \otimes w_1 - 1 \otimes 1)\\ &\qquad= 1 \otimes 1 - 1 \otimes 1\\ &\qquad= 0\end{aligned}$$

$$\begin{aligned}&(\pi_{\mathcal{I}_0(\mathbb{G})} \otimes \pi_{\mathcal{I}_0(\mathbb{G})}) \circ \Delta_{\mathcal{L}_0(\mathbb{G})}(yw_h - \chi(h)w_hy)\\ &\quad= (\pi_{\mathcal{I}_0(\mathbb{G})} \otimes \pi_{\mathcal{I}_0(\mathbb{G})})\big((1 \otimes y + y \otimes w_g)(w_h \otimes w_h) - \chi(h)(w_h \otimes w_h)(1 \otimes y + y \otimes w_g)\big)\\ &\quad= (\pi_{\mathcal{I}_0(\mathbb{G})} \otimes \pi_{\mathcal{I}_0(\mathbb{G})})\big(w_h \otimes yw_h + yw_h \otimes w_gw_h - \chi(h)w_h \otimes w_hy - \chi(h)w_hy \otimes w_hw_g\big)\\ &\quad= h \otimes xh + xh \otimes gh - \chi(h)h \otimes hx - \chi(h)hx \otimes hg\\ &\quad= h \otimes (xh - \chi(h)hx) + (xh - \chi(h)hx) \otimes gh\\ &\quad= h \otimes 0 + 0 \otimes gh\\ &\quad= 0\end{aligned}$$

Note que na álgebra $A(\mathbb{G})$ temos que:

$$\begin{aligned}(x \otimes g)(1 \otimes x) &= x \otimes gx\\ &= x \otimes (\chi(g)^{-1}xg)\\ &= \chi(g)^{-1}(1 \otimes x)(x \otimes g)\end{aligned}$$

Tomando $q = \chi(g)^{-1}$ e lembrando que $d = o(\chi(g))$, temos que q é uma d-ésima raíz primitiva da unidade em $\mathbb{K}$ e podemos usar os resultados de q-cálculo (ver Apêndice A) para $(x \otimes g)$ e $(1 \otimes x)$.

Temos:

$$
\begin{aligned}
(\pi_{\mathcal{I}_0(\mathbb{G})} \otimes \pi_{\mathcal{I}_0(\mathbb{G})}) \circ \Delta_{\mathcal{L}_0(\mathbb{G})}(y^d - \mu(1 - w_{g^d})) \\
&= (\pi_{\mathcal{I}_0(\mathbb{G})} \otimes \pi_{\mathcal{I}_0(\mathbb{G})})\big((1 \otimes y + y \otimes w_g)^d - \mu(1 \otimes 1 - w_{g^d} \otimes w_{g^d})\big) \\
&= (1 \otimes x + x \otimes g)^d - \mu(1 \otimes 1 - g^d \otimes g^d) \\
&\overset{\text{Corolário A.8}}{=} (1 \otimes x)^d + (x \otimes g)^d - \mu 1 \otimes 1 + \mu g^d \otimes g^d \\
&= 1 \otimes x^d + x^d \otimes g^d - \mu 1 \otimes 1 + \mu g^d \otimes g^d \\
&= 1 \otimes (\mu(1 - g^d)) + (\mu(1 - g^d)) \otimes g^d - \mu 1 \otimes 1 + \mu g^d \otimes g^d \\
&= \mu 1 \otimes 1 - \mu 1 \otimes g^d + \mu 1 \otimes g^d - \mu g^d \otimes g^d - \mu 1 \otimes 1 + \mu g^d \otimes g^d \\
&= 0
\end{aligned}
$$

Portanto $\Delta_{\mathcal{L}_0(\mathbb{G})}(\mathcal{I}_0(\mathbb{G})) \subset \ker(\pi \otimes \pi) = \mathcal{I}_0(\mathbb{G}) \otimes \mathcal{L}_0(\mathbb{G}) + \mathcal{L}_0(\mathbb{G}) \otimes \mathcal{I}_0(\mathbb{G})$.
Pela Proposição 1.48, temos que $A(\mathbb{G})$ é biálgebra e o morfismo projeção:

$$\pi_{\mathcal{I}_0(\mathbb{G})} \colon \mathcal{L}_0(\mathbb{G}) \to A(\mathbb{G})$$

é morfismo de biálgebras.

Vejamos que o conjunto $\{hx^i;\ h \in G, 0 \leq i \leq d-1\}$ é base de $A(\mathbb{G})$. Para isso, usaremos Lema do Diamante (ver Apêndice C). Os monômios da forma hx^i são os irredutíveis. Basta mostrar que todas as ambiguidades são resolúveis. São elas:

- (xh_1h_2): Neste caso, podemos utilizar primeiro a igualdade $xh_1 = \chi(h_1)h_1x$, obtendo:

$$
\begin{aligned}
xh_1h_2 &= \chi(h_1)h_1xh_2 \\
&= \chi(h_1)\chi(h_2)h_1h_2x
\end{aligned}
$$

  ou podemos considerar h_1h_2 como um elemento de G, obtendo:

$$x(h_1h_2) = \chi(h_1h_2)h_1h_2x$$

  Como χ é morfismo de grupos, temos que $\chi(h_1)\chi(h_2) = \chi(h_1h_2)$. Portanto esta ambiguidade é resolúvel.

- (x^dh): Neste caso, podemos utilizar primeiro a igualdade $xh = \chi(h)hx$, obtendo:

$$
\begin{aligned}
x^dh &= x^{d-1}xh \\
&= \chi(h)x^{d-1}hx \\
&\ \vdots \\
&= \chi(h)^d hx^d \\
&= \chi(h)^d \mu h(1 - g^d)
\end{aligned}
$$

  ou podemos utilizar primeiro a igualdade $x^d = \mu(1 - g^d)$, obtendo:

$$x^dh = \mu(1 - g^d)h$$

  Como g é central em G, temos que $(1 - g^d)h = h(1 - g^d)$, $\forall h \in G$. Pelas propriedades de conjunto de dados de grupo, se $\mu \neq 0$, então $\chi^d = 1$. Portanto esta ambiguidade é resolúvel.

- (x^{d+1}): Como $d = o(\chi(g))$, temos:

$$\begin{aligned} x\,x^d &= \mu x(1-g^d) \\ &= \mu(x - xg^d) \\ &= \mu(x - (\chi(g^d)g^d x) \end{aligned}$$

e

$$\begin{aligned} x^d x &= \mu(1-g^d)x \\ &= \mu(x - g^d x) \end{aligned}$$

Como $d = o(\chi(g))$ e χ é morfismo de grupos, temos que $\chi(g^d) = 1$. Portanto esta ambiguidade é resolúvel.

Portanto todas as ambiguidades são resolúveis.
Pelo Lema do Diamante, $\{hx^i;\ h \in G, 0 \le i \le d-1\}$ é base de $A(\mathbb{G})$. □

Proposição 2.6. *A biálgebra $A(\mathbb{G})$ é uma álgebra de Hopf com antípoda:*

$$\begin{aligned} S\colon A(\mathbb{G}) &\longrightarrow A(\mathbb{G}) \\ x &\longmapsto -xg^{-1} \\ h &\longmapsto h^{-1} \end{aligned}$$

Demonstração. Usaremos a demonstração proposta por Taft para o caso das álgebras de mesmo nome em [10]. Considere a função $\mathbb{K}$-linear:

$$\begin{aligned} f\colon \mathcal{V}_0(\mathbb{G}) &\longrightarrow A(\mathbb{G})^{op} \\ y &\longmapsto -xg^{-1} \\ w_h &\longmapsto h^{-1} \end{aligned}$$

Pela definição de álgebra tensorial, temos o morfismo de álgebras:

$$\begin{aligned} f'\colon \mathcal{L}_0(\mathbb{G}) &\longrightarrow A(\mathbb{G})^{op} \\ y &\longmapsto -xg^{-1} \\ w_h &\longmapsto h^{-1} \end{aligned}$$

Se $\mathcal{I}_0(\mathbb{G}) \subset \ker f'$, então pela Proposição B.7, existe um único morfismo de álgebras S que faz o seguinte diagrama comutar:

$$\begin{tikzcd} \mathcal{L}_0(\mathbb{G}) \arrow[rr, "f'"] \arrow[dr, "\pi_{\mathcal{I}_0(\mathbb{G})}"'] & & A(\mathbb{G})^{op} \\ & \mathcal{L}_0(\mathbb{G})/\mathcal{I}_0(\mathbb{G}) \arrow[ur, dotted, "S"'] & \end{tikzcd}$$

De fato, nos geradores de $\mathcal{I}_0(\mathbb{G})$, temos:

$$\begin{aligned} f'(w_{h_1}w_{h_2} - w_{h_1h_2}) &= f'(w_{h_1}w_{h_2}) - f'(w_{h_1h_2}) \\ &= m_{A(\mathbb{G})^{op}}(f'(w_{h_1}) \otimes f'(w_{h_2})) - (h_1h_2)^{-1} \\ &= h_2^{-1}h_1^{-1} - h_2^{-1}h_1^{-1} \\ &= 0 \end{aligned}$$

$$\begin{aligned} f'(w_1 - 1) &= f'(w_1) - f'(1) \\ &= 1^{-1} - 1 \\ &= 1 - 1 \\ &= 0 \end{aligned}$$

$$\begin{aligned} f'(yw_h - \chi(h)w_h y) &= f'(yw_h) - \chi(h)f'(w_h y) \\ &= m_{A(\mathbb{G})^{op}}(f'(y) \otimes f'(w_h)) - \chi(h)m_{A(\mathbb{G})^{op}}(f'(w_h) \otimes f'(y)) \\ &= h^{-1}(-xg^{-1}) - \chi(h)(-xg^{-1})h^{-1} \\ &= -\chi(g^{-1})h^{-1}g^{-1}x + \chi(g^{-1}h^{-1})\chi(h)g^{-1}h^{-1}x \\ &= -\chi(g^{-1})h^{-1}g^{-1}x + \chi(g^{-1}h^{-1}h)g^{-1}h^{-1}x \\ &= 0 \end{aligned}$$

$$\begin{aligned} f'(y^d - \mu(1 - w_{g^d})) &= f'(y)^d - \mu f'(1 - w_{g^d}) \\ &= (-xg^{-1})^d - \mu(1 - g^{-d}) \\ &= (-1)^d \overbrace{(xg^{-1}) \cdots (xg^{-1})}^{d\text{-vezes}} - \mu(1 - g^{-d}) \\ &= (-1)^d \chi(g^{-1})^{1+2+\cdots+d} g^{-d} x^d - \mu(1 - g^{-d}) \\ &= (-1)^d \chi(g^{-1})^{d(d+1)/2} \mu g^{-d}(1 - g^d) - \mu(1 - g^{-d}) \\ &= (-1)^d \chi(g^{-1})^{d(d+1)/2} \mu(g^{-d} - 1) - \mu(1 - g^{-d}) \\ &= (-1)^{d+1} \chi(g^{-1})^{d(d+1)/2} \mu(1 - g^{-d}) - \mu(1 - g^{-d}) \end{aligned}$$

Daí temos que:

- se d é ímpar, então $(d+1)/2$ é inteiro e temos que:

  $$\chi(g^{-1})^{d(d+1)/2} = (\chi(g)^d)^{-(d+1)/2} = 1$$

  e $(-1)^d = -1$.

  Logo:

  $$f'(y^d - \mu(1 - w_{g^d})) = 0$$

- se d é par, então $d/2$ é inteiro e temos que:

  $$\chi(g^{-1})^{d(d+1)/2} = (\chi(g)^{d+1})^{-d/2} = (\chi(g)^d \chi(g))^{-d/2} = \chi(g)^{-d/2}$$

  e $(-1)^d = 1$.

  Como $(\chi(g)^{-d/2})^2 = \chi(g)^{-d} = 1$, então $\chi(g)^{-d/2} = \pm 1$. Mas se $\chi(g)^{-d/2} = 1$, então $o(\chi(g)) < d$, o que é absurdo. Logo:

  $$\chi(g)^{-d/2} = -1$$

  e

  $$f'(y^d - \mu(1 - w_{g^d})) = 0$$

Portanto S é morfismo de álgebras entre $A(\mathbb{G})$ e $A(\mathbb{G})^{op}$. Pelo Corolário 1.58, precisamos mostrar que $A(\mathbb{G})^S = A(\mathbb{G})$. Pela Proposição 1.52, temos que $A(\mathbb{G})^S$ é subálgebra de $A(\mathbb{G})$.

Como $\Delta_{A(\mathbb{G})}(x) = 1 \otimes x + x \otimes g$, temos:

$$\begin{aligned} S(1)x + S(x)g &= 1x + (-xg^{-1})g \\ &= x - x \\ &= 0 \\ &= \varepsilon_{A(\mathbb{G})}(x)1 \end{aligned}$$

e

$$\begin{aligned} 1S(x) + xS(g) &= 1(-xg^{-1}) + xg^{-1} \\ &= 0 \\ &= \varepsilon_{A(\mathbb{G})}(x)1 \end{aligned}$$

Logo $x \in A(\mathbb{G})^S$.

Para cada $h \in G$ temos:

$$\begin{aligned} S(h)h &= h^{-1}h \\ &= 1 \\ &= \varepsilon_{A(\mathbb{G})}(h)1 \end{aligned}$$

e

$$\begin{aligned} hS(h) &= hh^{-1} \\ &= 1 \\ &= \varepsilon_{A(\mathbb{G})}(h)1 \end{aligned}$$

Logo $h \in A(\mathbb{G})^S$, $\forall h \in G$.

Portanto, como $\{x\} \cup \{h; h \in G\}$ gera $A(\mathbb{G})$ como álgebra, temos que $A(\mathbb{G})$ é subálgebra de $A(\mathbb{G})^S$, o que implica que $A(\mathbb{G})$ é álgebra de Hopf com antípoda S. □

Chamaremos $A(\mathbb{G})$ de álgebra de Hopf associada à $\mathbb{G}$. A prova de que toda álgebra de Hopf monomial não semi simples tem a forma de $A(\mathbb{G})$ é feita em [7]. Para verificar que $A(\mathbb{G})$ é não semi simples, basta tomar o ideal à esquerda $A(\mathbb{G})x$. Se $A(\mathbb{G}) = A(\mathbb{G})x \oplus I$ para algum ideal à esquerda I, então um elemento não nulo em I deve ser da forma $\sum \alpha_h h + mx$, onde m é um elemento qualquer de $A(\mathbb{G})$ e $\alpha_h \neq 0$ para algum $h \in G$. Mas, ao multiplicar por x, teremos um elemento não nulo que deve pertencer à $A(\mathbb{G})x$ e I. Absurdo. Portanto $A(\mathbb{G})$ não pode ser escrito como soma direta de ideais à esquerda sendo um deles $A(\mathbb{G})x$, ou seja, $A(\mathbb{G})$ não é semi simples.

Lema 2.7. *Seja $A(\mathbb{G})$ uma álgebra de Hopf associada à $\mathbb{G} = (G, g, \chi, \mu)$ e $0 \neq s \in A(\mathbb{G})$ um elemento qualquer. Então:*

1) se $\Delta_{A(\mathbb{G})}(s) = s \otimes s$, então $s \in G$;

2) se $\Delta_{A(\mathbb{G})}(s) = 1 \otimes s + s \otimes w$ com $w \in G$, então $s = r_1x + r_2(g-1)$ com $r_1, r_2 \in \mathbb{K}$ se $w = g$ e $s = r(w-1)$ com $r \in \mathbb{K}^*$ se $w \neq g$.

Demonstração. Pela Proposição 2.5, temos que $\{hx^i;\ h \in G, 0 \leq i \leq d-1\}$ é base de $A(\mathbb{G})$. Logo:

$$s = \sum_{h \in G} \sum_{i=0}^{d-1} \alpha_{h,i} hx^i$$

com $\alpha_{h,i} \in \mathbb{K}$, $\forall h \in G$, $i = 0, ..., d-1$. Além disso, tomando $q = \chi(g)^{-1}$, temos que:

$$\begin{aligned}(x \otimes g)(1 \otimes x) &= x \otimes gx \\ &= x \otimes \chi(g)^{-1} xg \\ &= \chi(g)^{-1}(1 \otimes x)(x \otimes g)\end{aligned}$$

e podemos usar q-cálculo para $(1 \otimes x)$ e $(x \otimes g)$. Temos:

$$\begin{aligned}\Delta_{A(\mathbb{G})}(s) &= \sum_{h \in G} \sum_{i=0}^{d-1} \alpha_{h,i} \Delta_{A(\mathbb{G})}(h) \Delta_{A(\mathbb{G})}(x)^i \\ &= \sum_{h \in G} \sum_{i=0}^{d-1} \alpha_{h,i} (h \otimes h)(x \otimes g + 1 \otimes x)^i \\ &\overset{\text{Proposição A.7}}{=} \sum_{h \in G} \sum_{i=0}^{d-1} \alpha_{h,i} (h \otimes h) \left(\sum_{t=0}^{i} \binom{i}{t}_q (x \otimes g)^{i-t} (1 \otimes x)^t \right) \\ &= \sum_{h \in G} \sum_{i=0}^{d-1} \sum_{t=0}^{i} \binom{i}{t}_q \alpha_{h,i} h x^{i-t} \otimes h g^{i-t} x^t\end{aligned}$$

1) Se $\Delta_{A(\mathbb{G})}(s) = s \otimes s$, então:

$$\sum_{h \in G} \sum_{i=0}^{d-1} \sum_{t=0}^{i} \binom{i}{t}_q \alpha_{h,i} h x^{i-t} \otimes h g^{i-t} x^t = \sum_{k,l \in G} \sum_{m,n=0}^{d-1} \alpha_{k,m} \alpha_{l,n} k x^m \otimes l x^n$$

Pela independência linear de $\{hx^i\}$ em $A(\mathbb{G})$, temos que, $\forall h \in G$, $i = 0, ..., d-1$ e $t = 0, ..., i$:

$$\binom{i}{t}_q \alpha_{h,i} h x^{i-t} \otimes h g^{i-t} x^t = \alpha_{h,i-t} \alpha_{hg^{i-t},t} h x^{i-t} \otimes h g^{i-t} x^t$$

Logo, para todo $h \in G$ e $i = 0, ..., d-1$, tomando $t = i$, temos:

$$\alpha_{h,i} = \alpha_{h,0} \alpha_{h,i}$$

Se $\alpha_{h,0} = 0$, $\forall h \in G$, então $\alpha_{h,i} = 0$, $\forall h \in G$ e $i = 0, ..., d-1$. Absurdo, pois $s \neq 0$.

Seja $h_0 \in G$ tal que $\alpha_{h_0,0} \neq 0$. Então tomando $i = t = 0$, temos:

$$\alpha_{h_0,0} = \alpha_{h_0,0} \alpha_{h_0,0}$$

Portanto $\alpha_{h_0,0} = 1$.

Pela independência linear de $\{hx^i\}$ em $A(\mathbb{G})$, como para qualquer $h \neq h_0$, o coeficiente do termo $h_0 \otimes h$ em $\Delta_{A(\mathbb{G})}(s)$ é 0 mas em $s \otimes s$ é $\alpha_{h_0,0}\alpha_{h,0}$, temos que $\alpha_{h,0} = 0$, $\forall h \neq h_0$. Mas como:

$$\alpha_{h,i} = \alpha_{h,0} \alpha_{h,i}$$

então $\alpha_{h,i} = 0$, $\forall h \neq h_0$ e $i = 0, ..., d-1$.

Como para qualquer $0 < i \leq d-1$, o coeficiente de $h_0 x^i \otimes h_0$ em $\Delta_{A(\mathbb{G})}(s)$ é 0 (pois x do lado esquerdo tem a mesma potência que g do lado direito) mas em $s \otimes s$ é $\alpha_{h_0,i}\alpha_{h_0,0}$, temos que $\alpha_{h_0,i} = 0$, $\forall i = 1, ..., d-1$.

Portanto $s = h_0 \in G$.

2) se $\Delta_{A(\mathbb{G})}(s) = 1 \otimes s + s \otimes w$, então:

$$\sum_{h\in G}\sum_{i=0}^{d-1}\sum_{t=0}^{i}\binom{i}{t}_q \alpha_{h,i} hx^{i-t} \otimes hg^{i-t}x^t = \sum_{k\in G}\sum_{j=0}^{d-1}\alpha_{k,j}(1 \otimes kx^j + kx^j \otimes w)$$

Se $i \geq 2$, para qualquer $h \in G$, podemos tomar $t = 1$ e o coeficiente de $hx^{i-1} \otimes hg^{i-1}x$ em $\Delta_{A(\mathbb{G})}(s)$ é $\binom{i}{1}_q \alpha_{h,i}$ mas em $1 \otimes s + s \otimes w$ é 0. Como $\binom{i}{1}_q \neq 0$, temos que $\alpha_{h,i} = 0$, $\forall h \in G$ e $i \geq 2$.

Logo, temos:

$$\sum_{h\in G}\big(\alpha_{h,0}h\otimes h+\alpha_{h,1}(hx\otimes hg+h\otimes hx)\big) = \sum_{k\in G}\big(\alpha_{k,0}(1\otimes k+k\otimes w)+\alpha_{k,1}(1\otimes kx+kx\otimes w)\big)$$

Pela independência linear de $\{hx^i\}$ em $A(\mathbb{G})$, podemos comparar os termos $a \otimes b$ com $a = 1$ ou $b = w$, da seguinte forma:

- com x^0:

$$\alpha_{1,0}1 \otimes 1 + \alpha_{w,0}w \otimes w = \alpha_{1,0}(1 \otimes 1 + 1 \otimes w) + \alpha_{w,0}(1 \otimes w + w \otimes w)$$

  Neste caso, como o coeficiente de $1 \otimes w$ do lado direito é $\alpha_{1,0} + \alpha_{w,0}$ e do lado esquerdo é 0, temos que $\alpha_{1,0} = -\alpha_{w,0}$.

- com x^1:

$$\alpha_{1,1}(1 \otimes x + x \otimes g) = \alpha_{1,1}(1 \otimes x + x \otimes w)$$

  Neste caso, se $w = g$, então $\alpha_{1,1}$ pode ser qualquer elemento de $\mathbb{K}$, mas se $w \neq g$, então $\alpha_{1,1} = 0$.

Portanto:

- se $w = g$, temos que $s = \alpha_{1,1}x + \alpha_{g,0}(g - 1)$;
- se $w \neq g$, temos que $s = \alpha_{w,0}(w - 1)$.

□

Proposição 2.8. *Sejam $\mathbb{G}, \mathbb{G}'$ dois conjuntos de dados de grupo e $A(\mathbb{G}), A(\mathbb{G}')$ suas respectivas álgebras de Hopf. Então $A(\mathbb{G}) \cong A(\mathbb{G}')$ se, e somente se, $\mathbb{G} \cong \mathbb{G}'$.*

Demonstração. ($\Rightarrow$) Seja $T\colon A(\mathbb{G}) \to A(\mathbb{G}')$ um isomorfismo de álgebras de Hopf. Como T é morfismo de coálgebras, temos que $\Delta_{A(\mathbb{G}')} \circ T = (T \otimes T) \circ \Delta_{A(\mathbb{G})}$. Logo, para cada $h \in G$ temos:

$$\begin{aligned}\Delta_{A(\mathbb{G}')} \circ T(h) &= (T \otimes T) \circ \Delta_{A(\mathbb{G})}(h)\\ &= (T \otimes T)(h \otimes h)\\ &= T(h) \otimes T(h)\end{aligned}$$

Pelo Lema 2.7, temos que $T(h) \in G'$, $\forall h \in G$. Como T é isomorfismo, temos que sua restrição à G é um monomorfismo de G à G'. Analogamente, se T^{-1} é a inversa de T, temos que T^{-1} restrito à G' é um monomorfismo de G' à G. Logo, T restrito à G é um isomorfismo de grupos entre G e G'.

Em x, temos:

$$\begin{aligned}
\Delta_{A(\mathbb{G}')} \circ T(x) &= (T \otimes T) \circ \Delta_{A(\mathbb{G})}(x) \\
&= (T \otimes T)(1 \otimes x + x \otimes g) \\
&= 1 \otimes T(x) + T(x) \otimes T(g)
\end{aligned}$$

Pelo Lema 2.7, se $T(g) \neq g'$, teríamos que $T(x) = r(T(g) - 1)$ com $r \in \mathbb{K}^*$.
Mas $T(r(g-1)) = r(T(g) - 1)$ e $r(g-1) \neq x$. Absurdo, pois T é monomorfismo.
Portanto $T(g) = g'$ e $T(x) = r_1 x + r_2(g' - 1)$ com $r_1, r_2 \in \mathbb{K}$.
Como T é morfismo de álgebras, temos que:

$$\begin{aligned}
T(xg) &= T(x)T(g) \\
&= (r_1 x + r_2(g' - 1))g' \\
&= r_1 x g' + r_2(g' - 1)g' \\
&= r_1 \chi'(g')g'x + r_2(g' - 1)g'
\end{aligned}$$

e

$$\begin{aligned}
T(\chi(g)gx) &= \chi(g)T(g)T(x) \\
&= \chi(g)g'(r_1 x + r_2(g' - 1)) \\
&= r_1 \chi(g)g'x + r_2 \chi(g)(g' - 1)g'
\end{aligned}$$

Como $T(xg) = T(\chi(g)gx)$ e $\chi(g) \neq 1$ (pois $1 < d = o(\chi(g))$), temos que $r_2 = 0$, o que implica $r_1 \neq 0$.

Para cada $h \in G$, temos:

$$\begin{aligned}
T(xh) &= T(x)T(h) \\
&= r_1 x T(h) \\
&= r_1 \chi'(T(h))T(h)x
\end{aligned}$$

e

$$\begin{aligned}
T(\chi(h)hx) &= \chi(h)T(h)T(x) \\
&= r_1 \chi(h)T(h)x
\end{aligned}$$

Como $T(xh) = T(\chi(h)hx)$, temos que $\chi' \circ T = \chi$.
Além disso, temos:

$$\begin{aligned}
T(x^d) &= T(x)^d \\
&= (r_1 x)^d \\
&= r_1^d x^d \\
&= r_1^d \mu'(1 - g'^d)
\end{aligned}$$

e

$$\begin{aligned}
T(\mu(1 - g^d)) &= \mu T((1 - g^d)) \\
&= \mu(1 - g'^d)
\end{aligned}$$

Como $T(x^d) = T(\mu(1 - g^d))$, temos que $\mu = r_1^d \mu'$.
Tomando u como a restrição de T à G e $w = r_1$, temos que $\mathbb{G}$ e $\mathbb{G}'$ são isomorfos.

($\Leftarrow$) Se $\mathbb{G} \cong \mathbb{G}'$, existem $\eta \in \mathbb{K}^*$ tal que $\mu = \eta^d \mu'$ e $u\colon G \to G'$ isomorfismo tal que $u(g) = g'$ e $\chi' \circ u = \chi$. Considere a função $\mathbb{K}$-linear:

$$\begin{aligned} f\colon A(\mathbb{G}) &\longrightarrow A(\mathbb{G}') \\ hx^i &\longmapsto \eta^i u(h) x^i \end{aligned}$$

Vejamos que f é morfismo de álgebras. De fato, como para todo $h \in G$, $\chi'(u(h)) = \chi(h)$, temos:

$$\begin{aligned} f(h_1 x^i h_2 x^j) &= f(\chi(h_2)^i h_1 h_2 x^{i+j}) \\ &= \chi(h_2)^i \eta^{i+j} u(h_1 h_2) x^{i+j} \\ &= \chi'(u(h_2))^i \eta^i \eta^j u(h_1) u(h_2) x^i x^j \\ &= \eta^i \eta^j u(h_1) x^i u(h_2) x^j \\ &= f(h_1 x^i) f(h_2 x^j) \end{aligned}$$

e como $u(1) = 1$:

$$\begin{aligned} f(1) &= u(1) \\ &= 1 \end{aligned}$$

Portanto f é morfismo de álgebras.

Vejamos que f é morfismo de coálgebras. De fato, como f, $\Delta_{A(\mathbb{G}')}$ e $\Delta_{A(\mathbb{G})}$ são morfismos de álgebras, temos:

$$\begin{aligned} \Delta_{A(\mathbb{G}')} \circ f(hx^i) &= \Delta_{A(\mathbb{G}')}(\eta^i u(h) x^i) \\ &= \eta^i (u(h) \otimes u(h))(1 \otimes x + x \otimes g)^i \\ &= (u(h) \otimes u(h))(1 \otimes \eta x + \eta x \otimes g)^i \\ &= (f(h) \otimes f(h))(f(1) \otimes f(x) + f(x) \otimes f(g))^i \\ &= (f \otimes f)((h \otimes h)(1 \otimes x + x \otimes g)^i) \\ &= (f \otimes f) \circ \Delta_{A(\mathbb{G})}(hx^i) \end{aligned}$$

e

$$\begin{aligned} \varepsilon_{A(\mathbb{G}')} \circ f(hx^i) &= \varepsilon_{A(\mathbb{G}')}(\eta^i u(h) x^i) \\ &= \eta^i \varepsilon_{A(\mathbb{G}')}(u(h)) \varepsilon_{A(\mathbb{G}')}(x)^i \end{aligned}$$

Assim temos que:

- se $i \neq 0$, como $\varepsilon_{A(\mathbb{G}')}(x) = 0$, temos que $\varepsilon_{A(\mathbb{G}')} \circ f(hx^i) = 0 = \varepsilon_{A(\mathbb{G})}(hx^i)$;
- se $i = 0$, então $\varepsilon_{A(\mathbb{G}')} \circ f(hx^i) = \varepsilon_{A(\mathbb{G}')}(u(h)) = 1 = \varepsilon_{A(\mathbb{G})}(hx^i)$.

Portanto f é morfismo de biálgebras. Como $\eta \neq 0$ e $u\colon G \to G'$ é isomorfismo, claramente temos que a função:

$$\begin{aligned} f'\colon A(\mathbb{G}') &\longrightarrow A(\mathbb{G}) \\ hx^i &\longmapsto \eta^{-i} u^{-1}(h) x^i \end{aligned}$$

é a inversa de f. Portanto f é isomorfismo. □

Agora apresentamos uma classificação dos conjuntos de dados de grupo, feita por Julien Bichon, [1]:

- **Tipo I:** Temos que $\mu = 0$, $d = o(\chi(g)) = o(g)$ e $\chi^d = 1$.
- **Tipo II:** Temos que $\mu = 0$, $d = o(\chi(g)) = o(g)$ e $\chi^d \neq 1$.
- **Tipo III:** Temos que $\mu = 0$, $d = o(\chi(g)) < o(g)$ e $\chi^d = 1$.
- **Tipo IV:** Temos que $\mu = 0$, $d = o(\chi(g)) < o(g)$, $\chi^d \neq 1$ e não existe $\sigma \in Z^2(G, \mathbb{K}^*)$ tal que $\chi(h)^d\sigma(h, g^d) = \sigma(g^d, h)$, $\forall h \in G$.
- **Tipo V:** Temos que $\mu = 0$, $d = o(\chi(g)) < o(g)$, $\chi^d \neq 1$ e existe $\sigma \in Z^2(G, \mathbb{K}^*)$ tal que $\chi(h)^d\sigma(h, g^d) = \sigma(g^d, h)$, $\forall h \in G$.
- **Tipo VI:** Temos que $\mu \neq 0$ (e consequentemente $d = o(\chi(g)) < o(g)$ e $\chi^{o(\chi(g))} = 1$).

Nos Teoremas 2.11 e 3.1, precisamos desta classificação, pois para cada tipo, existe uma abordagem apropriada para a descrição do conjunto dos objetos $A(\mathbb{G})$-Galois e do grupo dos objetos $A(\mathbb{G})$-biGalois.

Proposição 2.9. *Sejam $\mathbb{G} \cong \mathbb{G}'$. Então $\mathbb{G}$ e $\mathbb{G}'$ são do mesmo tipo.*

Demonstração. Sejam $\eta \in \mathbb{K}^*$ tal que $\mu = \eta^d\mu'$ e $u\colon G \to G'$ tal que $u(g) = g'$ e $\chi' \circ u = \chi$.

Logo, temos que $\mu = 0$ se, e somente se, $\mu' = 0$.

Como $u(g) = g'$ e $\chi' \circ u = \chi$, temos que:

$$d' = o(\chi'(g')) = o(\chi'(u(g))) = o(\chi(g)) = d$$

Como u é isomorfismo, temos que:

$$o(g) = o(u(g)) = o(g')$$

Além disso, temos que $\chi(h)^d = 1$, $\forall h \in G$ se, e somente se, $\chi'(u(h))^d = 1$, $\forall h \in G$. Mas como u é isomorfismo e $d = d'$, temos que $\chi'(u(h))^d = 1$, $\forall h \in G$ se, e somente se, $\chi'(h')^{d'} = 1$, $\forall h' \in G'$. Ou seja, $\chi^d = 1$ se, e somente se, $\chi'^{d'} = 1$.

Se existe $\sigma \in Z^2(G, \mathbb{K}^*)$ tal que:

$$\chi(h)^d\sigma(h, g^d) = \sigma(g^d, h),\ \forall h \in G$$

tome $\sigma' = \sigma \circ (u^{-1} \otimes u^{-1}) \in Z^2(G', \mathbb{K}^*)$. Então para todo $h' \in G'$:

$$\begin{aligned}
\chi'(h')^{d'}\sigma'(h', g'^{d'}) &= \chi'(u(u^{-1}(h')))^{d'}\sigma(u^{-1}(h'), u^{-1}(g'^{d'}))\\
&= \chi(u^{-1}(h'))^d\sigma(u^{-1}(h'), g^d)\\
&= \sigma(g^d, u^{-1}(h'))\\
&= \sigma(u^{-1}(g'^{d'}), u^{-1}(h'))\\
&= \sigma'(g'^{d'}, h')
\end{aligned}$$

Se existe $\sigma' \in Z^2(G', \mathbb{K}^*)$ tal que:

$$\chi'(h')^{d'}\sigma(h', g'^{d'}) = \sigma'(g'^{d'}, h'),\ \forall h' \in G'$$

tome $\sigma = \sigma' \circ (u \otimes u) \in Z^2(G, \mathbb{K}^*)$. Então para todo $h \in G$:

$$\begin{aligned}
\chi(h)^d\sigma(h, g^d) &= \chi(u^{-1}(u(h)))^d\sigma'(u(h'), u(g^d))\\
&= \chi'(u(h))^{d'}\sigma'(u(h), g'^{d'})\\
&= \sigma'(g'^{d'}, u(h))\\
&= \sigma'(u(g^d), u(h))\\
&= \sigma(g^d, h)
\end{aligned}$$

Portanto $\mathbb{G}$ e $\mathbb{G}'$ são do mesmo tipo. $\square$

Como consequência, temos a seguinte descrição para os automorfismos da álgebra de Hopf $A(\mathbb{G})$:

Proposição 2.10. *Seja $A(\mathbb{G})$ uma álgebra de Hopf associada a um conjunto de dados de grupo $\mathbb{G}$. Então se $\mathbb{G}$ é do tipo I ao V, temos uma correspondência bijetora:*

$$Aut_{Hopf}(A(\mathbb{G})) \cong Aut_{g,\chi}(G) \times \mathbb{K}^*$$

e se $\mathbb{G}$ é do tipo VI, temos uma correspondência bijetora:

$$Aut_{Hopf}(A(\mathbb{G})) \cong Aut_{g,\chi}(G) \times \Omega_d$$

onde $Aut_{g,\chi}(G) = \{u \in Aut_g(G); \chi \circ u = \chi\}$ e Ω_d é o grupo as d-ésimas raízes da unidade em $\mathbb{K}$.

Nas seções seguintes apresentaremos alguns resultados necessários para a demonstração do seguinte teorema:

Teorema 2.11. *Seja $\mathbb{G} = (G, g, \chi, \mu)$ um conjunto de dados de grupo. Então de acordo com o tipo de $\mathbb{G}$, temos a seguinte descrição para $Gal\big(A(\mathbb{G})\big)$:*

- ***Tipo I:*** $Gal\big(A(\mathbb{G})\big) \cong H^2(G, \mathbb{K}^*) \times \mathbb{K}$
- ***Tipo II e IV:*** $Gal\big(A(\mathbb{G})\big) \cong H^2(G, \mathbb{K}^*)$
- ***Tipo III, V e VI:*** $Gal\big(A(\mathbb{G})\big) \cong H^2(G, \mathbb{K}^*) \coprod H^2_{g^d,g^d}(G, \mathbb{K}^*)$

No teorema, $\coprod$ refere-se a união disjunta.

A demonstração para conjuntos de dados do tipo VI será feita no capítulo seguinte e segue um caminho totalmente diferente dos demais.

Nas seções seguintes deste capítulo, assuma $\mathbb{G} = (G, g, \chi)$ um conjunto de dados de grupo ($\mu = 0$), $d = o(\chi(g)) > 1$ e $q = \chi(g)^{-1}$.

2.2 Os objetos $A(\mathbb{G})$-Galois $A_{\sigma,a,\Psi}(\mathbb{G})$

Nesta seção apresentaremos a álgebra $A_{\sigma,a,\Psi}(\mathbb{G})$, um tipo especial de objeto $A(\mathbb{G})$-Galois, e sua relação com os demais objetos $A(\mathbb{G})$-Galois.

Definição 2.12. *Sejam $\mathcal{V}(\mathbb{G})$ o espaço vetorial com base B,onde $B = \{Y\} \bigcup \{W_h;\, h \in G\}$ e $\mathcal{L}(\mathbb{G})$ a álgebra tensorial sobre $\mathcal{V}(\mathbb{G})$. Para $\sigma \in Z^2(G, \mathbb{K}^*)$, $a \in \mathbb{K}$ e uma função $\Psi\colon G \to \mathbb{K}$, definimos $\mathcal{I}_{\sigma,a,\Psi}(\mathbb{G})$ como o ideal bilateral de $\mathcal{L}(\mathbb{G})$ gerado por:*

$$\begin{gathered}\big(W_{h_1}W_{h_2} - \sigma(h_1,h_2)W_{h_1h_2}\big)_{h_1,h_2\in G}\\ W_1 - 1\\ \big(YW_h - \chi(h)W_hY - \Psi(h)W_{gh}\big)_{h\in G}\\ Y^d - aW_{g^d}\end{gathered}$$

Chamaremos de $A_{\sigma,a,\Psi}(\mathbb{G})$ a álgebra quociente $\mathcal{L}(\mathbb{G})/\mathcal{I}_{\sigma,a,\Psi}(\mathbb{G})$, X a classe lateral de Y e T_h a classe lateral de W_h em $A_{\sigma,a,\Psi}(\mathbb{G})$.

No caso $\Psi \equiv 0$, denotaremos $\mathcal{I}_{\sigma,a,\Psi}(\mathbb{G})$ por $\mathcal{I}_{\sigma,a}(\mathbb{G})$ e $A_{\sigma,a,\Psi}(\mathbb{G})$ por $A_{\sigma,a}(\mathbb{G})$.

Lema 2.13. *O espaço vetorial $\mathcal{V}(\mathbb{G})$ é $A(\mathbb{G})$-comódulo com estrutura dada por:*

$$\begin{aligned}\rho_{\mathcal{V}(\mathbb{G})}\colon \mathcal{V}(\mathbb{G}) &\longrightarrow \mathcal{V}(\mathbb{G}) \otimes A(\mathbb{G})\\ Y &\longmapsto 1 \otimes x + Y \otimes g\\ W_h &\longmapsto W_h \otimes h\end{aligned}$$

Demonstração. Vejamos que $\rho_{\mathcal{V}(\mathbb{G})}$ satisfaz os seguintes diagramas comutativos:

$$\begin{tikzcd}
\mathcal{V}(\mathbb{G}) \arrow[r, "\rho_{\mathcal{V}(\mathbb{G})}"] \arrow[d, "\rho_{\mathcal{V}(\mathbb{G})}"'] & \mathcal{V}(\mathbb{G}) \otimes A(\mathbb{G}) \arrow[d, "\rho_{\mathcal{V}(\mathbb{G})} \otimes A(\mathbb{G})"] \\
\mathcal{V}(\mathbb{G}) \otimes A(\mathbb{G}) \arrow[r, "\mathcal{V}(\mathbb{G}) \otimes \Delta_{A(\mathbb{G})}"] & \mathcal{V}(\mathbb{G}) \otimes A(\mathbb{G}) \otimes A(\mathbb{G})
\end{tikzcd}$$

$$\begin{tikzcd}
\mathcal{V}(\mathbb{G}) \arrow[rr, "\rho_{\mathcal{V}(\mathbb{G})}"] \arrow[dr, "\cong"'] & & \mathcal{V}(\mathbb{G}) \otimes A(\mathbb{G}) \arrow[dl, "\mathcal{V}(\mathbb{G}) \otimes \varepsilon_{A(\mathbb{G})}"] \\
& \mathcal{V}(\mathbb{G}) \otimes \mathbb{K} &
\end{tikzcd}$$

Pela linearidade de $\rho_{\mathcal{V}(\mathbb{G})}$, basta verificar nos elementos da base de $\mathcal{V}(\mathbb{G})$. Temos que:

$$\begin{aligned}
\left(\rho_{\mathcal{V}(\mathbb{G})} \otimes A(\mathbb{G})\right) \circ \rho_{\mathcal{V}(\mathbb{G})}(Y) &= \left(\rho_{\mathcal{V}(\mathbb{G})} \otimes A(\mathbb{G})\right)(1 \otimes x + Y \otimes g) \\
&= \rho_{\mathcal{V}(\mathbb{G})}(1) \otimes x + \rho_{\mathcal{V}(\mathbb{G})}(Y) \otimes g \\
&= 1 \otimes 1 \otimes x + 1 \otimes x \otimes g + Y \otimes g \otimes g \\
&= 1 \otimes (1 \otimes x + x \otimes g) + Y \otimes g \otimes g \\
&= 1 \otimes \Delta_{A(\mathbb{G})}(x) + Y \otimes \Delta_{A(\mathbb{G})}(g) \\
&= \left(\mathcal{V}(\mathbb{G}) \otimes \Delta_{A(\mathbb{G})}\right)(1 \otimes x + Y \otimes g) \\
&= \left(\mathcal{V}(\mathbb{G}) \otimes \Delta_{A(\mathbb{G})}\right) \circ \rho_{\mathcal{V}(\mathbb{G})}(Y)
\end{aligned}$$

$$\begin{aligned}
\left(\mathcal{V}(\mathbb{G}) \otimes \varepsilon_{A(\mathbb{G})}\right) \circ \rho_{\mathcal{V}(\mathbb{G})}(Y) &= \left(\mathcal{V}(\mathbb{G}) \otimes \varepsilon_{A(\mathbb{G})}\right)(1 \otimes x + Y \otimes g) \\
&= 1 \otimes \varepsilon_{A(\mathbb{G})}(x) + Y \otimes \varepsilon_{A(\mathbb{G})}(g) \\
&= Y \otimes 1
\end{aligned}$$

$$\begin{aligned}
\left(\rho_{\mathcal{V}(\mathbb{G})} \otimes A(\mathbb{G})\right) \circ \rho_{\mathcal{V}(\mathbb{G})}(W_h) &= \left(\rho_{\mathcal{V}(\mathbb{G})} \otimes A(\mathbb{G})\right)(W_h \otimes h) \\
&= \rho_{\mathcal{V}(\mathbb{G})}(W_h) \otimes h \\
&= W_h \otimes h \otimes h \\
&= W_h \otimes \Delta_{A(\mathbb{G})}(h) \\
&= \left(\mathcal{V}(\mathbb{G}) \otimes \Delta_{A(\mathbb{G})}\right)(W_h \otimes h) \\
&= \left(\mathcal{V}(\mathbb{G}) \otimes \Delta_{A(\mathbb{G})}\right) \circ \rho_{\mathcal{V}(\mathbb{G})}(W_h)
\end{aligned}$$

$$\begin{aligned}
\left(\mathcal{V}(\mathbb{G}) \otimes \varepsilon_{A(\mathbb{G})}\right) \circ \rho_{\mathcal{V}(\mathbb{G})}(W_h) &= \left(\mathcal{V}(\mathbb{G}) \otimes \varepsilon_{A(\mathbb{G})}\right)(W_h \otimes h) \\
&= W_h \otimes \varepsilon_{A(\mathbb{G})}(h) \\
&= W_h \otimes 1
\end{aligned}$$

Como as duas últimas equações não dependem de h, verificamos para todos os elementos da base de $\mathcal{V}(\mathbb{G})$. Portanto $\mathcal{V}(\mathbb{G})$ é $A(\mathbb{G})$-comódulo. $\square$

Pela Teorema 1.10, temos o seguinte resultado: A álgebra $\mathcal{L}(\mathbb{G})$ é $A(\mathbb{G})$-comódulo álgebra com coação dada por:

$$\begin{aligned}
\rho_{\mathcal{L}(\mathbb{G})} \colon \mathcal{L}(\mathbb{G}) &\longrightarrow \mathcal{L}(\mathbb{G}) \otimes A(\mathbb{G}) \\
Y &\longmapsto 1 \otimes x + Y \otimes g \\
W_h &\longmapsto W_h \otimes h
\end{aligned}$$

Lema 2.14. *O conjunto* $\{T_h X^i;\, h \in G, 0 \leq i \leq d-1\}$ *gera* $A_{\sigma,a,\Psi}(\mathbb{G})$.

Demonstração. Um elemento $\alpha \in A_{\sigma,a,\Psi}(\mathbb{G})$ é da forma $\alpha = \beta + \mathcal{I}_{\sigma,a,\Psi}(\mathbb{G})$, onde $\beta \in \mathcal{L}(\mathbb{G})$. Este β por sua vez é da forma $\beta = \sum_{j=0}^{n} \lambda_j Q_{j,1} Q_{j,2} \cdots Q_{j,m_j}$, com $\lambda_j \in \mathbb{K}$, $n, m_j \in \mathbb{N}$ e $Q_{k,l} \in \{Y\} \bigcup \{W_h | h \in G\}$.

Se, para algum k e algum l tivermos $Q_{k,l} = W_{h_1}$ e $Q_{k,l+1} = W_{h_2}$, podemos substituir $Q_{k,l}Q_{k,l+1}$ por $\sigma(h_1, h_2)W_{h_1h_2}$ no produtório permanecendo na classe de equivalência α, pois $W_{h_1}W_{h_2} - \sigma(h_1, h_2)W_{h_1h_2} \in \mathcal{I}_{\sigma,a,\Psi}(\mathbb{G})$.

Usando este argumento recursivamente, podemos substituir o representante de α por um elemento de $\mathcal{L}(\mathbb{G})$ que possui apenas monômios da forma $Y^{n_1}W_{h_1}Y^{n_2}W_{h_2} \cdots Y^{n_s}W_{h_s}Y^{n_{s+1}}$, ou seja, que é produto de potências de Y e algum W_h, alternadamente.

Se, para algum k e algum l tivermos $Q_{k,l} = Y$ e $Q_{k,l+1} = W_h$, podemos substituir $Q_{k,l}Q_{k,l+1}$ por $\chi(h)W_hY + \Psi(h)T_{gh}$ no produtório permanecendo na classe de equivalência α, pois $YW_h - \chi(h)W_hY - \Psi(h)W_{gh} \in \mathcal{I}_{\sigma,a,\Psi}(\mathbb{G})$.

Usando este argumento recursivamente juntamente com o argumento anterior, podemos substituir o representante de α por um elemento de $\mathcal{L}(\mathbb{G})$ que possui apenas monômios da forma W_hY^n.

Se em algum monômio tivermos Y^n, com $n \geq d$, podemos substituir cada Y^d por aW_{g^d} no produtório permanecendo na classe de equivalência α, pois $Y^d - aWg^d \in \mathcal{I}_{\sigma,a,\Psi}(\mathbb{G})$.

Portanto, podemos escolher um representante de α que possui apenas monômios da forma W_hY^i, com $h \in G$ e $0 \leq i \leq d-1$. Ou seja, podemos escrever α como combinação linear de elementos da forma T_hX^i, com $h \in G$ e $0 \leq i \leq d-1$. □

Proposição 2.15. *A álgebra $A_{\sigma,a,\Psi}(\mathbb{G})$ tem estrutura de $A(\mathbb{G})$-comódulo álgebra à direita com coação $\rho\colon A_{\sigma,a,\Psi}(\mathbb{G}) \to A_{\sigma,a,\Psi}(\mathbb{G}) \otimes A(\mathbb{G})$ definida por:*

$$\begin{aligned} \rho(X) &= 1 \otimes x + X \otimes g, \\ \rho(T_h) &= T_h \otimes h, \qquad \forall h \in G. \end{aligned}$$

Além disso, as seguintes afirmações são equivalentes:

1) *$A_{\sigma,a,\Psi}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois à direita.*

2) *$\dim A_{\sigma,a,\Psi}(\mathbb{G}) = |G|d$ e o conjunto $\{T_hX^i;\ h \in G, 0 \leq i \leq d-1\}$ é uma base de $A_{\sigma,a,\Psi}(\mathbb{G})$ sobre $\mathbb{K}$.*

3) *$A_{\sigma,a,\Psi}(\mathbb{G})$ é uma álgebra não nula.*

Demonstração. Vejamos que $\rho_{\mathcal{L}(\mathbb{G})}\left(\mathcal{I}_{\sigma,a,\Psi}(\mathbb{G})\right) \subset \mathcal{I}_{\sigma,a,\Psi}(\mathbb{G}) \otimes A(\mathbb{G})$.

De fato, nos geradores de $\mathcal{I}_{\sigma,a,\Psi}(\mathbb{G})$ temos que:

$$\begin{aligned} \rho_{\mathcal{L}(\mathbb{G})}\left(W_{h_1}W_{h_2} - \sigma(h_1,h_2)W_{h_1h_2}\right) &= \left(W_{h_1} \otimes h_1\right)\left(W_{h_2} \otimes h_2\right) - \sigma(h_1,h_2)\left(W_{h_1h_2} \otimes h_1h_2\right) \\ &= W_{h_1}W_{h_2} \otimes h_1h_2 - \sigma(h_1,h_2)W_{h_1h_2} \otimes h_1h_2 \\ &= \left(W_{h_1}W_{h_2} - \sigma(h_1,h_2)W_{h_1h_2}\right) \otimes h_1h_2 \end{aligned}$$

$$\begin{aligned} \rho_{\mathcal{L}(\mathbb{G})}\left(W_1 - 1\right) &= W_1 \otimes 1 - 1 \otimes 1 \\ &= \left(W_1 - 1\right) \otimes 1 \end{aligned}$$

$$\begin{aligned} \rho_{\mathcal{L}(\mathbb{G})}\left(YW_h - \chi(h)W_hY - \Psi(h)W_{gh}\right) &= \left(1 \otimes x + Y \otimes g\right)\left(W_h \otimes h\right) \\ &\quad - \chi(h)\left(W_h \otimes h\right)\left(1 \otimes x + Y \otimes g\right) - \Psi(h)\left(W_{gh} \otimes gh\right) \\ &= W_h \otimes xh + YW_h \otimes gh - \chi(h)W_h \otimes hx \\ &\quad - \chi(h)W_hY \otimes hg - \Psi(h)W_{gh} \otimes gh \\ &= \left(YW_h - \chi(h)W_hY - \Psi(h)W_{gh}\right) \otimes gh \\ &\quad + W_h \otimes \left(xh - \chi(h)hx\right) \\ &= \left(YW_h - \chi(h)W_hY - \Psi(h)W_{gh}\right) \otimes gh \end{aligned}$$

Para o elemento $Y^d - aW_{g^d}$, a fim de simplificar a verificação, podemos utilizar o seguinte fato: Seja $\pi\colon \mathcal{L}(\mathbb{G}) \to A_{\sigma,a,\Psi}(\mathbb{G})$ o morfismo projeção. Como $\ker \pi = \mathcal{I}_{\sigma,a,\Psi}(\mathbb{G})$, então $\ker(\pi \otimes A(\mathbb{G})) = \mathcal{I}_{\sigma,a,\Psi}(\mathbb{G}) \otimes A(\mathbb{G})$.

Note que na álgebra $A_{\sigma,a,\Psi}(\mathbb{G})$ temos que:

$$\begin{aligned}(X \otimes g)(1 \otimes x) &= X \otimes gx \\ &= X \otimes (\chi(g)^{-1} xg) \\ &= \chi(g)^{-1}(1 \otimes x)(X \otimes g)\end{aligned}$$

Tomando $q = \chi(g)^{-1}$, que é uma d-ésima raíz primitiva da unidade em $\mathbb{K}$, podemos usar os resultados de q-cálculo para $(X \otimes g)$ e $(1 \otimes x)$.

Temos:

$$\begin{aligned}(\pi \otimes A(\mathbb{G})) \circ \rho_{\mathcal{L}(\mathbb{G})}\left(Y^d - aW_{g^d}\right) &= (\pi \otimes A(\mathbb{G}))\big((1 \otimes x + Y \otimes g)^d - aW_{g^d} \otimes g^d\big) \\ &= (1 \otimes x + X \otimes g)^d - aT_{g^d} \otimes g^d \\ &\overset{\text{Corolário A.8}}{=} (1 \otimes x)^d + (X \otimes g)^d - aT_{g^d} \otimes g^d \\ &= 1 \otimes x^d + X^d \otimes g^d - aT_{g^d} \otimes g^d \\ &= \left(X^d - aT_{g^d}\right) \otimes g^d \\ &= 0\end{aligned}$$

Portanto $\rho_{\mathcal{L}(\mathbb{G})}\left(Y^d - aW_{g^d}\right) \in \ker(\pi \otimes A(\mathbb{G})) = \mathcal{I}_{\sigma,a,\Psi}(\mathbb{G}) \otimes A(\mathbb{G})$.

Pelo Corolário 1.14, $A_{\sigma,a,\Psi}(\mathbb{G})$ é $A(\mathbb{G})$-comódulo álgebra com coação ρ dada por:

$$\begin{aligned}\rho(X) &= 1 \otimes x + X \otimes g, \\ \rho(T_h) &= T_h \otimes h, \qquad \forall h \in G.\end{aligned}$$

- 1)$\Rightarrow$ 2) Como $\dim A(\mathbb{G}) < \infty$, temos que $A_{\sigma,a,\Psi}(\mathbb{G})$ é fendido. Logo, existe um 2-cociclo τ tal que $A_{\sigma,a,\Psi}(\mathbb{G}) \cong {}_\tau A(\mathbb{G})$. Assim, temos que $\dim A_{\sigma,a,\Psi}(\mathbb{G}) = \dim {}_\tau A(\mathbb{G}) = |G|d$. Pelo Lema 2.14, temos que $\{T_h X^i;\ h \in G, 0 \le i \le d-1\}$ é gerador e portanto é base.

- 2)$\Rightarrow$ 3) Como $\dim A_{\sigma,a,\Psi}(\mathbb{G}) \neq 0$, temos que $A_{\sigma,a,\Psi}(\mathbb{G})$ é álgebra não nula.

- 3)$\Rightarrow$ 1) Vejamos que $A_{\sigma,a,\Psi}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois, ou seja, que a função κ_r é sobrejetora. Para isso, vamos usar indução sobre o índice i nos elementos hx^i da base de $A(\mathbb{G})$ e o fato de κ_r ser $A_{\sigma,a,\Psi}(\mathbb{G})$-linear à esquerda.

  Para cada $h \in G$ temos:

$$\begin{aligned}\kappa_r(1 \otimes T_h) &= 1\rho(T_h) \\ &= (T_h \otimes h)\end{aligned}$$

  e pela $A_{\sigma,a,\Psi}(\mathbb{G})$-linearidade à esquerda temos:

$$\begin{aligned}\kappa_r\left(\sigma(h^{-1},h)^{-1} T_{h^{-1}} \otimes T_h\right) &= \sigma(h^{-1},h)^{-1} T_{h^{-1}} \kappa_r(1 \otimes T_h) \\ &= \sigma(h^{-1},h)^{-1} T_{h^{-1}}(T_h \otimes h) \\ &= \sigma(h^{-1},h)^{-1} \sigma(h^{-1},h) T_{h^{-1}h} \otimes h \\ &= 1 \otimes h\end{aligned}$$

  A fim de melhorar a notação nas equações seguintes, denotaremos por ξ_h o elemento $\sigma(h^{-1},h)^{-1} T_{h^{-1}} \otimes T_h \in A_{\sigma,a,\Psi}(\mathbb{G}) \otimes A_{\sigma,a,\Psi}(\mathbb{G})$, $\forall h \in G$.

Assim, para todo $h \in G$ e $1 \leq i \leq d$ temos que:

$$\begin{aligned}
\kappa_r\left(\xi_h X^i\right) &= \kappa_r\left(\sigma(h^{-1},h)^{-1}T_{h^{-1}} \otimes T_h X^i\right) \\
&= \sigma(h^{-1},h)^{-1}T_{h^{-1}}\rho\left(T_h X^i\right) \\
&= \sigma(h^{-1},h)^{-1}T_{h^{-1}}\rho\left(T_h\right)\rho\left(X\right)^i \\
&= \sigma(h^{-1},h)^{-1}T_{h^{-1}}\left(T_h \otimes h\right)\left(X \otimes g + 1 \otimes x\right)^i \\
&= \left(1 \otimes h\right)\left(X \otimes g + 1 \otimes x\right)^i \\
&\overset{\text{Proposição A.7}}{=} \left(1 \otimes h\right)\left(\sum_{t=0}^{i}\binom{i}{t}_q \left(X \otimes g\right)^{i-t}\left(1 \otimes x\right)^t\right) \\
&= \sum_{t=0}^{i}\binom{i}{t}_q X^{i-t} \otimes hg^{i-t}x^t
\end{aligned}$$

Observação 2.16. *Note que poderíamos ter utilizado $q = \chi(g)$ e $(1 \otimes x + X \otimes g)^i$ sem afetar o resultado final, pois a soma é comutativa, mas desta forma, após utilizar a Proposição A.7, apareceríam termos da forma $hx^{i-t}g^t$ do lado direito do produto direto, que não estão na forma reduzida.*

Vejamos que $1 \otimes hx$ está na imagem de κ_r para todo $h \in G$:

$$\begin{aligned}
\kappa_r\left(\xi_h X - X\xi_{hg}\right) &= \kappa_r\left(\xi_h X\right) - X\kappa_r\left(\xi_{hg}\right) \\
&= 1 \otimes hx + X \otimes hg - X \otimes hg \\
&= 1 \otimes hx
\end{aligned}$$

Assuma que $1 \otimes hx^t$ está na imagem de κ_r, $\forall h \in G$ e $0 \leq t \leq i-1$.

Seja $\eta_{h,t} \in A_{\sigma,a,\Psi}(\mathbb{G}) \otimes A_{\sigma,a,\Psi}(\mathbb{G})$ tal que $\kappa_r\left(\eta_{h,t}\right) = 1 \otimes hx^t$. Então:

$$\begin{aligned}
\kappa_r\left(\xi_h X^i - \sum_{t=0}^{i-1}\binom{i}{t}_q X^{i-t}\eta_{hg^{i-t},t}\right) &= \kappa_r\left(\xi_h X^i\right) - \sum_{t=0}^{i-1}\binom{i}{t}_q X^{i-t}\kappa_r\left(\eta_{hg^{i-t},t}\right) \\
&= \sum_{t=0}^{i}\binom{i}{t}_q X^{i-t} \otimes hg^{i-t}x^t \\
&\quad - \sum_{t=0}^{i-1}\binom{i}{t}_q X^{i-t}\left(1 \otimes hg^{i-t}x^t\right) \\
&= 1 \otimes hx^i
\end{aligned}$$

Logo, todos os elementos da forma $1 \otimes hx^i$ estão na imagem de κ_r.

Como κ_r é $A_{\sigma,a,\Psi}(\mathbb{G})$-linear à esquerda, temos que κ_r é sobrejetora.

Assim, temos que:

$$\begin{aligned}
(\dim A_{\sigma,a,\Psi}(\mathbb{G}))(\dim A_{\sigma,a,\Psi}(\mathbb{G})) &= \dim\left(A_{\sigma,a,\Psi}(\mathbb{G}) \otimes A_{\sigma,a,\Psi}(\mathbb{G})\right) \\
&\geq \dim\left(A_{\sigma,a,\Psi}(\mathbb{G}) \otimes A(\mathbb{G})\right) \\
&= (\dim A_{\sigma,a,\Psi}(\mathbb{G}))(\dim A(\mathbb{G}))
\end{aligned}$$

Como $A_{\sigma,a,\Psi}(\mathbb{G})$ é algebra não-nula, $\dim A_{\sigma,a,\Psi}(\mathbb{G}) \neq 0$. Portanto:

$$\dim A_{\sigma,a,\Psi}(\mathbb{G}) \geq \dim A(\mathbb{G}) = |G|d$$

Pelo Lema 2.14, temos que $\dim A_{\sigma,a,\Psi}(\mathbb{G}) \leq |G|d$. Portanto:

$$\dim A_{\sigma,a,\Psi}(\mathbb{G}) = |G|d = \dim A(\mathbb{G})$$

e

$$\dim A_{\sigma,a,\Psi}(\mathbb{G}) \otimes A_{\sigma,a,\Psi}(\mathbb{G}) = \dim A_{\sigma,a,\Psi}(\mathbb{G}) \otimes A(\mathbb{G})$$

Logo a função κ_r é isomorfismo, o que implica que $A_{\sigma,a,\Psi}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois.

□

Lema 2.17. *Sejam $\mathbb{G} = (G, g, \chi, \mu)$ um conjunto de dados de grupo, $A(\mathbb{G})$ a álgebra de Hopf associada a $\mathbb{G}$, σ um 2-cociclo sobre $A(\mathbb{G})$ e $\rho\colon {}_\sigma A(\mathbb{G}) \to {}_\sigma A(\mathbb{G}) \otimes A(\mathbb{G})$ a coação de $A(\mathbb{G})$ sobre ${}_\sigma A(\mathbb{G})$. Se $\rho(s) = s \otimes \eta$ com $\eta \in G$, então $s = \lambda\eta$ para algum $\lambda \in \mathbb{K}$.*

Demonstração. Como espaços vetoriais, temos que ${}_\sigma A(\mathbb{G}) = A(\mathbb{G})$.

Logo, $\{hx^i;\ h \in G, 0 \leq i \leq d-1\}$ é base de ${}_\sigma A(\mathbb{G})$ e temos que:

$$s = \sum_{h\in G}\sum_{i=0}^{d-1} \alpha_{h,i} h x^i$$

com $\alpha_{h,i} \in \mathbb{K}$, $\forall h \in G$ e $0 \leq i \leq d-1$.

Por um lado estamos supondo que:

$$\begin{aligned}\rho(s) &= s \otimes \eta\\ &= \sum_{h\in G}\sum_{i=0}^{d-1} \alpha_{h,i} h x^i \otimes \eta\end{aligned}$$

Por outro lado, temos que:

$$\begin{aligned}\rho(s) &= \rho\Big(\sum_{h\in G}\sum_{i=0}^{d-1} \alpha_{h,i} h x^i\Big)\\ &= \sum_{h\in G}\sum_{i=0}^{d-1} \alpha_{h,i} \rho(h)\rho(x)^i\\ &= \sum_{h\in G}\sum_{i=0}^{d-1} \alpha_{h,i} (h\otimes h)(1\otimes x + x\otimes g)^i\\ &\overset{\text{Proposição A.7}}{=} \sum_{h\in G}\sum_{i=0}^{d-1}\sum_{t=0}^{i} \binom{i}{t}_q \alpha_{h,i}(h\otimes h)(x\otimes g)^{i-t}(1\otimes x)^t\\ &= \sum_{h\in G}\sum_{i=0}^{d-1}\sum_{t=0}^{i} \binom{i}{t}_q \alpha_{h,i} h \cdot_\sigma \overbrace{x \cdot_\sigma x \cdot_\sigma \cdots \cdot_\sigma x}^{i-t\text{-vezes}} \otimes h g^{i-t} x^t\end{aligned}$$

Assim temos:

$$\sum_{l\in G}\sum_{j=0}^{d-1} \alpha_{l,j} h l x^j \otimes \eta = \sum_{h\in G}\sum_{i=0}^{d-1}\sum_{t=0}^{i} \binom{i}{t}_q \alpha_{h,i} h \cdot_\sigma \overbrace{x \cdot_\sigma x \cdot_\sigma \cdots \cdot_\sigma x}^{i-t\text{-vezes}} \otimes h g^{i-t} x^t$$

Sabemos que $\{hx^i;\ h \in G, 0 \leq i \leq d-1\}$ é base de $A(\mathbb{G})$ e de ${}_\sigma A(\mathbb{G})$. Vamos estudar os termos que possuem a mesma potência de x do lado direito.

A potência x^{d-1} aparece apenas para $i = t = d-1$. Temos:

$$0 = \sum_{h \in G} \binom{d-1}{d-1}_q \alpha_{h,d-1} h \otimes h x^{d-1}, \ \forall h \in G$$

Logo $\alpha_{h,d-1} = 0$, $\forall h \in G$.

Suponha que para algum $1 < j \leq d-1$ temos que $\alpha_{h,i} = 0$, $\forall i \geq j$, $\forall h \in G$. A potência x^{j-1} aparece apenas para $i = t = j-1$. Temos:

$$0 = \sum_{h \in G} \binom{j-1}{j-1}_q \alpha_{h,j-1} h \otimes h x^{j-1}, \ \forall h \in G$$

Logo $\alpha_{h,j-1} = 0$, $\forall h \in G$.

Assim temos que:

1) se $i > 0$, então $\alpha_{h,i} = 0$, $\forall h \in G$;

2) se $i = 0$, então $\alpha_{h,0} = 0$ para $h \neq \eta$.

Portanto, $s = \alpha_{\eta,0}\eta$. □

Lema 2.18. *Seja T um objeto $A(\mathbb{G})$-Galois à direita. Então existem $\sigma \in Z^2(G, \mathbb{K}^*)$, $a \in \mathbb{K}$ e $\Psi\colon G \to \mathbb{K}$ tais que $T \cong A_{\sigma,a,\Psi}(\mathbb{G})$ como $A(\mathbb{G})$-comódulo álgebras à direita.*

Demonstração. Como $\dim A(\mathbb{G}) < \infty$, pelo Teorema 1.96, temos que T é fendido. Logo, existe um 2-cociclo σ e $\varphi\colon {}_\sigma A(\mathbb{G}) \to T$ isomorfismo de $A(\mathbb{G})$-comódulo álgebras.

Considere o morfismo $f\colon \mathcal{V}(\mathbb{G}) \to {}_\sigma A(\mathbb{G})$ dado por $f(Y) = x$ e $f(W_h) = h$, $\forall h \in G$. Vejamos que f é morfismo de $A(\mathbb{G})$-comódulos:

$$\begin{aligned} \rho_{{}_\sigma A(\mathbb{G})} \circ f(Y) &= \rho_{{}_\sigma A(\mathbb{G})}(x) \\ &= 1 \otimes x + x \otimes g \\ &= (f \otimes {}_\sigma A(\mathbb{G}))\,(1 \otimes x + Y \otimes g) \\ &= (f \otimes {}_\sigma A(\mathbb{G})) \circ \rho_{\mathcal{V}(\mathbb{G})}(Y) \end{aligned}$$

e para todo $h \in G$:

$$\begin{aligned} \rho_{{}_\sigma A(\mathbb{G})} \circ f(W_h) &= \rho_{{}_\sigma A(\mathbb{G})}(h) \\ &= h \otimes h \\ &= (f \otimes {}_\sigma A(\mathbb{G}))\,(W_h \otimes h) \\ &= (f \otimes {}_\sigma A(\mathbb{G})) \circ \rho_{\mathcal{V}(\mathbb{G})}(W_h) \end{aligned}$$

Portanto f é morfismo de $A(\mathbb{G})$-comódulos à direita. Seja $f'\colon \mathcal{L}(\mathbb{G}) \to {}_\sigma A(\mathbb{G})$ o morfismo de $A(\mathbb{G})$-comódulo álgebras dada pelo Corolário 1.11. Vejamos que existem $a \in \mathbb{K}$ e $\Psi\colon G \to \mathbb{K}$ tais que $\mathcal{I}_{\sigma',a,\Psi}(\mathbb{G}) \subset \ker f'$, onde σ' é a restrição de σ à G.

Para qualquer $a \in \mathbb{K}$ e $\Psi\colon G \to \mathbb{K}$, temos para $h_1, h_2 \in G$:

$$\begin{aligned} f'(W_{h_1}W_{h_2} - \sigma(h_1,h_2)W_{h_1h_2}) &= h_1 \cdot_\sigma h_2 - \sigma(h_1,h_2)h_1h_2 \\ &= \sigma(h_1,h_2)h_1h_2 - \sigma(h_1,h_2)h_1h_2 \\ &= 0 \end{aligned}$$

e

$$\begin{aligned} f'(W_1 - 1) &= 1 - 1 \\ &= 0 \end{aligned}$$

Logo, precisamos apenas verificar que existem a e Ψ tais que $YW_h - \chi(h)W_hY - \Psi(h)W_{gh}$, $Y^d - aW_{g^d} \in \ker f'$. Como f' é morfismo de $A(\mathbb{G})$-comódulo álgebras, temos que, para cada $h \in G$:

$$\begin{aligned}
\rho_{\sigma A(\mathbb{G})} \circ f'(YW_h - \chi(h)W_hY) &= (f' \otimes A(\mathbb{G})) \circ \rho_{\mathcal{L}(\mathbb{G})}(YW_h - \chi(h)W_hY) \\
&= (f' \otimes A(\mathbb{G}))\big((1 \otimes x + Y \otimes g)(W_h \otimes h) \\
&\quad - \chi(h)(W_h \otimes h)(1 \otimes x + Y \otimes g)\big) \\
&= (1 \otimes x + x \otimes g)(h \otimes h) - \chi(h)(h \otimes h)(1 \otimes x + x \otimes g) \\
&= h \otimes xh + x \cdot_\sigma h \otimes gh - \chi(h)h \otimes hx - \chi(h)h \cdot_\sigma x \otimes hg \\
&= (x \cdot_\sigma h - \chi(h)h \cdot_\sigma x) \otimes gh \\
&= f'(YW_h - \chi(h)W_hY) \otimes gh
\end{aligned}$$

Pela Lema 2.17, temos que $f'(YW_h - \chi(h)W_hY) = \lambda_h gh$, para algum $\lambda_h \in \mathbb{K}$. Mas $f'(\lambda_h W_{gh}) = \lambda_h gh$. Logo, pela linearidade de f', temos que:

$$f'(YW_h - \chi(h)W_hY - \lambda_h W_{gh}) = 0$$

Tome a função $\Psi\colon G \to \mathbb{K}$ dada por $\Psi(h) = \lambda_h, \forall h \in G$.

Além disso, temos que:

$$\begin{aligned}
\rho_{\sigma A(\mathbb{G})} \circ f'(Y^d) &= (f' \otimes A(\mathbb{G})) \circ \rho_{\mathcal{L}(\mathbb{G})}(Y^d) \\
&= (f' \otimes A(\mathbb{G}))\big((1 \otimes x + Y \otimes g)^d\big) \\
&\overset{\text{Corolário A.8}}{=} (f' \otimes A(\mathbb{G}))\big(1 \otimes x^d + Y^d \otimes g^d\big) \\
&= f'(1) \otimes x^d + f'(Y^d) \otimes g^d \\
&= 1 \otimes x^d + f'(Y^d) \otimes g^d
\end{aligned}$$

Como estamos assumindo $\mu = 0$, temos que $x^d = 0$ em $A(\mathbb{G})$. Logo, temos que:

$$\rho_{\sigma A(\mathbb{G})} \circ f'(Y^d) = f'(Y^d) \otimes g^d$$

Pela Lema 2.17, temos que $f'(Y^d) = ag^d$, para algum $a \in \mathbb{K}$. Mas $f'(aW_{g^d}) = ag^d$. Logo, pela linearidade de f', temos que:

$$f'(Y^d - aW_{g^d}) = 0$$

Portanto, encontramos uma constante $a \in \mathbb{K}$ e uma função $\Psi\colon G \to \mathbb{K}$ tais que:

$$\mathcal{I}_{\sigma',a,\Psi}(\mathbb{G}) \subset \ker f'$$

Tome o morfismo $\bar{f}\colon A_{\sigma',a,\Psi}(\mathbb{G}) \to {}_\sigma A(\mathbb{G})$ dado pelo Corolário 1.15. Como $\bar{f}(X) = x$ e $\bar{f}(T_h) = h$, $\forall h \in G$, temos que $\bar{f}$ é sobrejetor. Como $\dim {}_\sigma A(\mathbb{G}) = |G|d \neq 0$, temos que $A_{\sigma',a,\Psi}(\mathbb{G})$ é álgebra não nula.

A composição $\varphi \circ \bar{f}\colon A_{\sigma',a,\Psi}(\mathbb{G}) \to T$ é morfismo de $A(\mathbb{G})$-comódulo álgebras. Pela Proposição 2.15, $A_{\sigma',a,\Psi}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois o que implica que $\varphi \circ \bar{f}$ é isomorfismo. □

2.3 Os objetos $A(\mathbb{G})$-Galois $A_{\sigma,a}(\mathbb{G})$

Nesta seção mostraremos que o Ψ é dispensável, ou seja, que todo objeto $A(\mathbb{G})$-Galois é isomorfo à uma álgebra do tipo $A_{\sigma,a}(\mathbb{G})$.

Lema 2.19. *Se $A_{\sigma,a,\Psi}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois à direita, então $\forall h \in G$ temos:*

$$\Psi(h) = \Psi(g)\left(\sigma(g,h) - \chi(h)\sigma(h,g)\right)\sigma(g,g)^{-1}\left(1 - \chi(g)\right)^{-1}$$

Demonstração. Como $A_{\sigma,a,\Psi}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois, pela Proposição 2.15, temos que o conjunto $\{T_h X^i;\, h \in G, 0 \leq i \leq d-1\}$ é base linear de $A_{\sigma,a,\Psi}(\mathbb{G})$. Então para todo $h_1, h_2 \in G$ temos:

$$\begin{aligned}
\Psi(h_1h_2)T_{h_1h_2g} &= XT_{h_1h_2} - \chi(h_1h_2)T_{h_1h_2}X \\
&= \sigma(h_1,h_2)^{-1}XT_{h_1}T_{h_2} - \chi(h_1h_2)T_{h_1h_2}X \\
&= \sigma(h_1,h_2)^{-1}\left(\chi(h_1)T_{h_1}X + \Psi(h_1)T_{h_1g}\right)T_{h_2} - \chi(h_1h_2)T_{h_1h_2}X \\
&= \sigma(h_1,h_2)^{-1}\left(\chi(h_1)T_{h_1}\left(\chi(h_2)T_{h_2}X + \Psi(h_2)T_{h_2g}\right) + \Psi(h_1)T_{h_1g}T_{h_2}\right) \\
&\quad - \chi(h_1h_2)T_{h_1h_2}X \\
&= \sigma(h_1,h_2)^{-1}\chi(h_1)\chi(h_2)T_{h_1}T_{h_2}X + \sigma(h_1,h_2)^{-1}\chi(h_1)\Psi(h_2)T_{h_1}T_{h_2g} \\
&\quad + \sigma(h_1,h_2)^{-1}\Psi(h_1)\sigma(h_1g,h_2)T_{h_1h_2g} - \chi(h_1h_2)T_{h_1h_2}X \\
&= \sigma(h_1,h_2)^{-1}\left(\chi(h_1)\Psi(h_2)\sigma(h_1,h_2g) + \Psi(h_1)\sigma(h_1g,h_2)\right)T_{h_1h_2g}
\end{aligned}$$

o que implica que:

$$\Psi(h_1h_2) = \sigma(h_1,h_2)^{-1}\left(\chi(h_1)\Psi(h_2)\sigma(h_1,h_2g) + \Psi(h_1)\sigma(h_1g,h_2)\right)$$

Então, para cada $h \in G$ temos:

$$\Psi(hg) = \sigma(h,g)^{-1}\big(\chi(h)\Psi(g)\sigma(h,g^2) + \Psi(h)\sigma(hg,g)\big)$$

e

$$\Psi(gh) = \sigma(g,h)^{-1}\big(\chi(g)\Psi(h)\sigma(g,hg) + \Psi(g)\sigma(g^2,h)\big)$$

Como g é central, temos que $\Psi(hg) = \Psi(gh)$. Logo:

$$\sigma(h,g)^{-1}\big(\chi(h)\Psi(g)\sigma(h,g^2) + \Psi(h)\sigma(hg,g)\big) = \sigma(g,h)^{-1}\big(\chi(g)\Psi(h)\sigma(g,hg) + \Psi(g)\sigma(g^2,h)\big)$$

Além disso, σ é 2-cociclo, o que implica que:

$$\begin{aligned}
\sigma(h,g)^{-1}\sigma(h,g^2) &= \sigma(hg,g)\sigma(g,g)^{-1} \\
\sigma(g,h)^{-1}\sigma(g^2,h) &= \sigma(g,gh)\sigma(g,g)^{-1} \\
\sigma(h,g)^{-1}\sigma(gh,g) &= \sigma(g,hg)\sigma(g,h)^{-1}
\end{aligned}$$

Logo:

$$\Psi(h)\sigma(h,g)^{-1}\sigma(gh,h)\left(1-\chi(g)\right) = \Psi(g)\left(\sigma(g,gh) - \chi(h)\sigma(hg,g)\right)\sigma(g,g)^{-1}$$

Isolando $\Psi(h)$, temos:

$$\Psi(h) = \Psi(g)\left(\sigma(g,h) - \chi(h)\sigma(h,g)\right)\sigma(g,g)^{-1}\left(1-\chi(g)\right)^{-1}$$

□

Lema 2.20. *Seja $\sigma \in Z^2(G,\mathbb{K}^*)$, $a \in \mathbb{K}$ e $\Psi\colon G \to \mathbb{K}$ tais que $A_{\sigma,a,\Psi}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois à direita. Então existe $a' \in \mathbb{K}$ tal que $A_{\sigma,a,\Psi}(\mathbb{G}) \cong A_{\sigma,a'}(\mathbb{G})$ como $A(\mathbb{G})$-comódulo álgebras à direita.*

Demonstração. Pela Proposição 2.15, para qualquer $a' \in \mathbb{K}$, $\big(A_{\sigma,a'}(\mathbb{G}),\rho\big)$ é $A(\mathbb{G})$-comódulo. Para qualquer $\lambda \in \mathbb{K}$, a função:

$$\begin{aligned}
f\colon \mathcal{V}(\mathbb{G}) &\longrightarrow A_{\sigma,a'}(\mathbb{G}) \\
Y &\longmapsto X + \lambda T_g \\
W_h &\longmapsto T_h
\end{aligned}$$

é morfismo de $A(\mathbb{G})$-comódulos. De fato, temos:

$$\begin{aligned}\rho\circ f(Y) &= \rho(X+\lambda T_g)\\ &= 1\otimes x + X\otimes g + \lambda T_g\otimes g\\ &= 1\otimes x + (X+\lambda T_g)\otimes g\\ &= (f\otimes A(\mathbb{G}))(1\otimes x) + (f\otimes A(\mathbb{G}))(Y\otimes g)\\ &= (f\otimes A(\mathbb{G}))\circ \rho_{\mathcal{V}(\mathbb{G})}(Y)\end{aligned}$$

e para cada $h\in G$:

$$\begin{aligned}\rho\circ f(W_h) &= \rho(T_h)\\ &= T_h\otimes h\\ &= (f\otimes A(\mathbb{G}))(W_h\otimes h)\\ &= (f\otimes A(\mathbb{G}))\circ \rho_{\mathcal{V}(\mathbb{G})}(W_h)\end{aligned}$$

Então f é morfismo de $A(\mathbb{G})$-comódulos.

Considere o morfismo de $A(\mathbb{G})$-comódulo álgebras $f'\colon \mathcal{L}(\mathbb{G})\to A_{\sigma,a'}(\mathbb{G})$ dado pelo Corolário 1.11. Para $h_1,h_2,h\in G$, temos:

$$\begin{aligned}f'\left(W_{h_1}W_{h_2}-\sigma(h_1,h_2)W_{h_1h_2}\right) &= T_{h_1}T_{h_2}-\sigma(h_1,h_2)T_{h_1h_2}\\ &= 0\end{aligned}$$

$$\begin{aligned}f'\left(W_1-1\right) &= T_1-1\\ &= 0\end{aligned}$$

$$\begin{aligned}f'\big(YW_h-\chi(h)W_hY-\Psi(h)W_{gh}\big) &= (X+\lambda T_g)T_h-\chi(h)T_h(X+\lambda T_g)-\Psi(h)T_{gh}\\ &= XT_h+\lambda T_gT_h-\chi(h)T_hX-\chi(h)\lambda T_hT_g-\Psi(h)T_{gh}\\ &= XT_h-\chi(h)T_hX+\big(\lambda\sigma(g,h)-\chi(h)\lambda\sigma(h,g)-\Psi(h)\big)T_{gh}\\ &= \big(\lambda\sigma(g,h)-\chi(h)\lambda\sigma(h,g)-\Psi(h)\big)T_{gh}\end{aligned}$$

$$\begin{aligned}f'\big(Y^d-aW_{g^d}\big) &= (X+\lambda T_g)^d-aT_{g^d}\\ &\overset{\text{Corolário A.8}}{=} X^d+\lambda^d(T_g)^d-aT_{g^d}\\ &= \big(a'+\lambda^d\sigma(g,g)\cdots\sigma(g,g^{d-1})-a\big)T_{g^d}\end{aligned}$$

Para que $\mathcal{I}_{\sigma,a,\Psi}(\mathbb{G})\subset\ker f'$, precisamos de:

$$\lambda\sigma(g,h)-\chi(h)\lambda\sigma(h,g)-\Psi(h)=0,\quad \forall h\in G$$

e

$$a'+\lambda^d\sigma(g,g)\cdots\sigma(g,g^{d-1})-a=0$$

Mas para cada $h\in G$ temos:

$$\begin{aligned}\lambda &= \Psi(h)\big(\sigma(g,h)-\chi(h)\sigma(h,g)\big)^{-1}\\ &\overset{\text{Lema 2.19}}{=} \Psi(g)\big(\sigma(g,h)-\chi(h)\sigma(h,g)\big)\sigma(g,g)^{-1}\left(1-\chi(g)\right)^{-1}\big(\sigma(g,h)-\chi(h)\sigma(h,g)\big)^{-1}\\ &= \Psi(g)\sigma(g,g)^{-1}\left(1-\chi(g)\right)^{-1}\end{aligned}$$

Portanto existem $\lambda,a'\in\mathbb{K}$ tais que $\mathcal{I}_{\sigma,a,\Psi}(\mathbb{G})\subset\ker f'$. Pelo Corolário 1.15, temos que existe $\bar f\colon A_{\sigma,a,\Psi}(\mathbb{G})\to A_{\sigma,a'}(\mathbb{G})$ morfismo de $A(\mathbb{G})$-comódulo álgebras. Mas, como $A_{\sigma,a,\Psi}(\mathbb{G})$ e $A_{\sigma,a'}(\mathbb{G})$ são objetos $A(\mathbb{G})$-Galois, segue que $\bar f$ é isomorfismo. $\square$

Teorema 2.21. *Seja T um objeto $A(\mathbb{G})$-Galois à direita. Então existem $\sigma \in Z^2(G,\mathbb{K}^*)$ e $a \in \mathbb{K}$ tais que $T \cong A_{\sigma,a}(\mathbb{G})$ como $A(\mathbb{G})$-comódulo álgebras à direita.*

Demonstração. Pelo Lema 2.18, temos que existem $\sigma \in Z^2(G,\mathbb{K}^*)$, $b \in \mathbb{K}$ e $\Psi : G \to \mathbb{K}$ tais que $T \cong A_{\sigma,b,\Psi}(\mathbb{G})$.

Pelo Lema 2.20, temos que existe $a \in \mathbb{K}$ tal que $A_{\sigma,b,\Psi}(\mathbb{G}) \cong A_{\sigma,a}(\mathbb{G})$.

Portanto temos que $T \cong A_{\sigma,a}(\mathbb{G})$. □

2.4 Caracterização dos objetos $A(\mathbb{G})$-Galois

Nesta seção, na Proposição 2.23, mostraremos como verificar se dois objetos $A(\mathbb{G})$-Galois são isomorfos e, na Proposição 2.24, apresentaremos uma equação que verifica se uma álgebra $A_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois.

Lema 2.22. *Sejam $A_{\sigma,a}(\mathbb{G})$ um objeto $A(\mathbb{G})$-Galois e $s \in A_{\sigma,a}(\mathbb{G})$ um elemento qualquer. Temos que:*

1) se para algum $\eta \in G$ temos $\rho(s) = s \otimes \eta$, então existe $\lambda \in \mathbb{K}$ tal que $s = \lambda\,\eta$;

2) se $\rho(s) = 1 \otimes x + s \otimes g$, então existe $\lambda \in \mathbb{K}$ tal que $s = X + \lambda T_g$.

Demonstração. Como $A_{\sigma,a}(\mathbb{G})$ é um objeto $A(\mathbb{G})$-Galois, pela Proposição 2.15, temos que $\{T_h X^i;\ h \in G, 0 \le i \le d-1\}$ é base de $A_{\sigma,a}(\mathbb{G})$. Logo:

$$s = \sum_{h\in G}\sum_{i=0}^{d-1} \alpha_{h,i} T_h X^i$$

com $\alpha_{h,i} \in \mathbb{K}$, $\forall h \in G$, $i = 0, ..., d-1$. Além disso, tomando $q = \chi(g)^{-1}$, temos que:

$$\begin{aligned}
\rho(s) &= \sum_{h\in G}\sum_{i=0}^{d-1} \alpha_{h,i}\rho(T_h)\rho(X)^i \\
&= \sum_{h\in G}\sum_{i=0}^{d-1} \alpha_{h,i}(T_h \otimes h)(X \otimes g + 1 \otimes x)^i \\
&\overset{\text{Proposição A.7}}{=} \sum_{h\in G}\sum_{i=0}^{d-1} \alpha_{h,i}(T_h \otimes h)\left(\sum_{t=0}^{i}\binom{i}{t}_q (X\otimes g)^{i-t}(1\otimes x)^t\right) \\
&= \sum_{h\in G}\sum_{i=0}^{d-1}\sum_{t=0}^{i}\binom{i}{t}_q \alpha_{h,i} T_h X^{i-t} \otimes h g^{i-t} x^t
\end{aligned}$$

1) Se para algum $\eta \in G$ temos $\rho(s) = s \otimes \eta$, então:

$$\sum_{l\in G}\sum_{j=0}^{d-1} \alpha_{l,j} T_l X^j \otimes \eta = \sum_{h\in G}\sum_{i=0}^{d-1}\sum_{t=0}^{i}\binom{i}{t}_q \alpha_{h,i} T_h X^{i-t} \otimes h g^{i-t} x^t$$

Temos que $\{T_h X^i;\ h \in G, 0 \le i \le d-1\}$ é base de $A_{\sigma,a}(\mathbb{G})$ e $\{hx^i;\ h \in G, 0 \le i \le d-1\}$ é base de $A(\mathbb{G})$. Vamos estudar os termos da soma que possuem a mesma potência de x à direita do produto tensorial. Como $\eta \in G$, potências diferentes de x^0 não aparecem do lado esquerdo da equação.

A potência x^{d-1} aparece apenas para $i = t = d-1$. Temos:

$$0 = \sum_{h \in G} \binom{d-1}{d-1}_q \alpha_{h,d-1} T_h \otimes hx^{d-1}$$

Pela independência linear de $\{T_h\}_{h \in G}$ em $A_{\sigma,a}(\mathbb{G})$ e $\{hx^i\}$ em $A(\mathbb{G})$, temos que:

$$\alpha_{h,d-1} = 0, \ \forall h \in G$$

Suponha que para algum $1 < j \leq d-1$ temos que $\alpha_{h,i} = 0$, $\forall i \geq j$, $\forall h \in G$. A potência x^{j-1} aparece apenas para $i = t = j-1$. Temos:

$$0 = \sum_{h \in G} \binom{j-1}{j-1}_q \alpha_{h,j-1} T_h \otimes hx^{j-1}$$

Pela independência linear de $\{T_h\}_{h \in G}$ em $A_{\sigma,a}(\mathbb{G})$ e $\{hx^i\}$ em $A(\mathbb{G})$, temos que:

$$\alpha_{h,j-1} = 0, \ \forall h \in G$$

Assim temos que, se $i > 0$, então $\alpha_{h,i} = 0$, $\forall h \in G$. Logo ficamos com a seguinte equação:

$$\sum_{l \in G} \alpha_{l,0} T_l \otimes \eta = \sum_{h \in G} \binom{0}{0}_q \alpha_{h,0} T_h \otimes h$$

Portanto, se $h \neq \eta$, então $\alpha_{h,0} = 0$.Logo:

$$s = \alpha_{\eta,0}\eta$$

2) se $\rho(s) = 1 \otimes x + s \otimes g$, então:

$$1 \otimes x + \sum_{l \in G} \sum_{j=0}^{d-1} \alpha_{l,j} T_l X^j \otimes g = \sum_{h \in G} \sum_{i=0}^{d-1} \sum_{t=0}^{i} \binom{i}{t}_q \alpha_{h,i} T_h X^{i-t} \otimes hg^{i-t} x^t$$

Temos que $\{T_h X^i;\ h \in G, 0 \leq i \leq d-1\}$ é base de $A_{\sigma,a}(\mathbb{G})$ e $\{hx^i;\ h \in G, 0 \leq i \leq d-1\}$ é base de $A(\mathbb{G})$. Vamos estudar os termos da soma que possuem a mesma potência de x à direita do produto tensorial. Potências diferentes de x^0 e x^1 não aparecem do lado esquerdo da equação.

A potência x^{d-1} aparece apenas para $i = t = d-1$. Temos:

$$0 = \sum_{h \in G} \binom{d-1}{d-1}_q \alpha_{h,d-1} T_h \otimes hx^{d-1}$$

Logo $\alpha_{h,d-1} = 0$, $\forall h \in G$.

Suponha que para algum $2 < j \leq d-1$ temos que $\alpha_{h,i} = 0$, $\forall i \geq j$, $\forall h \in G$. A potência x^{j-1} aparece apenas para $i = t = j-1$. Temos:

$$0 = \sum_{h \in G} \binom{j-1}{j-1}_q \alpha_{h,j-1} T_h \otimes hx^{j-1}$$

Logo $\alpha_{h,j-1} = 0$, $\forall h \in G$.

Assim temos que, se $i > 1$, então $\alpha_{h,i} = 0$, $\forall h \in G$. Logo, ficamos com a seguinte equação:

$$1 \otimes x + \sum_{l \in G} \alpha_{l,0} T_l \otimes g + \alpha_{l,1} T_l X \otimes g = \sum_{h \in G} \alpha_{h,0} T_h \otimes h + \binom{1}{0}_q \alpha_{h,1} T_h X \otimes hg + \alpha_{h,1} T_h \otimes hx$$

Temos que, se $h \neq 1$ e $h \neq g$, então $\alpha_{h,0} = \alpha_{h,1} = 0$. Se $h = 1$, então $\alpha_{h,0} = 0$. Se $h = g$, então $\alpha_{h,1} = 0$.

Portanto $s = \alpha_{1,1} X + \alpha_{g,0} T_g$.

Vejamos que $\alpha_{1,1} = 1$. De fato, temos:

$$\begin{aligned} \rho(s) &= \alpha_{1,1} \rho(X) + \alpha_{g,0} \rho(T_g) \\ &= \alpha_{1,1} (1 \otimes x + X \otimes g) + \alpha_{g,0} (T_g \otimes g) \\ &= \alpha_{1,1} \otimes x + s \otimes g \end{aligned}$$

Portanto $\alpha_{1,1} = 1$ e $s = X + \alpha_{g,0} T_g$.

□

Proposição 2.23. *Sejam $\sigma, \tau \in Z^2(G, \mathbb{K}^*)$ e $a, b \in \mathbb{K}$ tais que $A_{\sigma,a}(\mathbb{G})$ e $A_{\tau,b}(\mathbb{G})$ são objetos $A(\mathbb{G})$-Galois. Então $A_{\sigma,a}(\mathbb{G})$ e $A_{\tau,b}(\mathbb{G})$ são isomorfos como $A(\mathbb{G})$-comódulo álgebras se, e somente se, existe $\theta \colon G \to \mathbb{K}^*$ com $\theta(1) = 1$ tal que:*

$$\sigma = \partial(\theta)\tau \ \text{ e } b = a\theta(g^d)$$

Demonstração. ($\Rightarrow$) Sejam $f \colon A_{\sigma,a}(\mathbb{G}) \to A_{\tau,b}(\mathbb{G})$ um isomorfismo de $A(\mathbb{G})$-comódulo álgebras, ρ_a e ρ_b as coações de $A(\mathbb{G})$ sobre $A_{\sigma,a}(\mathbb{G})$ e $A_{\tau,b}(\mathbb{G})$ respectivamente. Temos que:

$$\begin{aligned} \rho_b \circ f(X) &= (f \otimes A(\mathbb{G})) \circ \rho_a(X) \\ &= (f \otimes A(\mathbb{G}))(1 \otimes x + X \otimes g) \\ &= 1 \otimes x + f(X) \otimes g \end{aligned}$$

e para cada $h \in G$:

$$\begin{aligned} \rho_b \circ f(T_h) &= (f \otimes A(\mathbb{G})) \circ \rho_a(T_h) \\ &= (f \otimes A(\mathbb{G}))(T_h \otimes h) \\ &= f(T_h) \otimes h \end{aligned}$$

Pelo Lema 2.22, temos que existem $\lambda \in \mathbb{K}$ e uma função $\theta \colon G \to \mathbb{K}^*$ tais que:

$$f(X) = X + \lambda T_g \text{ e } f(T_h) = \theta(h) T_h, \forall h \in G$$

Temos que $1 = f(1) = f(T_1) = \theta(1) T_1 = \theta(1)$. Além disso, dados $h_1, h_2 \in G$, temos:

$$\begin{aligned} f(T_{h_1} T_{h_2}) &= f(T_{h_1}) f(T_{h_2}) \\ &= \theta(h_1)\theta(h_2) T_{h_1} T_{h_2} \\ &= \theta(h_1)\theta(h_2)\tau(h_1, h_2) T_{h_1 h_2} \end{aligned}$$

$$\begin{aligned} f(\sigma(h_1, h_2) T_{h_1 h_2}) &= \sigma(h_1, h_2) f(T_{h_1 h_2}) \\ &= \sigma(h_1, h_2)\theta(h_1 h_2) T_{h_1 h_2} \end{aligned}$$

Logo, temos que:

$$\theta(h_1)\theta(h_2)\tau(h_1, h_2) = \sigma(h_1, h_2)\theta(h_1 h_2)$$

que implica:

$$\sigma(h_1,h_2)\tau(h_1,h_2)^{-1} = \theta(h_1)\theta(h_1h_2)^{-1}\theta(h_2)$$

Ou seja, $\sigma = \partial(\theta)\tau$. Vejamos que $b = a\theta(g^d)$. De fato:

$$\begin{aligned} f(XT_g) &= f(X)f(T_g) \\ &= (X+\lambda T_g)(\theta(g)T_g) \\ &= \theta(g)XT_g + \lambda\theta(g)T_gT_g \\ &= \theta(g)XT_g + \lambda\theta(g)\tau(g,g)T_{g^2} \end{aligned}$$

e

$$\begin{aligned} f(\chi(g)T_gX) &= \chi(g)f(T_g)f(X) \\ &= \chi(g)(\theta(g)T_g)(X+\lambda T_g) \\ &= \chi(g)\theta(g)T_gX + \chi(g)\lambda\theta(g)T_gT_g \\ &= \chi(g)\theta(g)T_gX + \chi(g)\lambda\theta(g)\tau(g,g)T_{g^2} \end{aligned}$$

Como $f(XT_g) = f(\chi(g)T_gX)$ e $1 < d = 0(\chi(g))$, temos que $\chi(g) \neq 1$ e $\lambda = 0$. Logo temos:

$$bT_{g^d} = X^d = f(X)^d = f(X^d) = f(aT_{g^d}) = a\theta(g^d)T_{g^d}$$

Portanto $b = a\theta(g^d)$.

($\Leftarrow$) Considere o morfismo de $A(\mathbb{G})$-comódulos $f\colon \mathcal{V}(\mathbb{G}) \to A_{\tau,b}(\mathbb{G})$ dado por:

$$f(Y) = X \text{ e } f(W_h) = \theta(h)T_h,\ \forall h \in G$$

e $f'\colon \mathcal{L}(\mathbb{G}) \to A_{\tau,b}(\mathbb{G})$ o morfismo de $A(\mathbb{G})$-comódulo álgebras dado pelo Corolário 1.11. Vejamos que $\sigma = \partial(\theta)\tau$ e $b = a\theta(g^d)$ implicam que $\mathcal{I}_{\sigma,a}(\mathbb{G}) \subset \ker f'$. De fato, temos:

$$\begin{aligned} f'(W_{h_1}W_{h_2} - \sigma(h_1,h_2)W_{h_1h_2}) &= f'(W_{h_1})f'(W_{h_2}) - \sigma(h_1,h_2)f'(W_{h_1h_2}) \\ &= \theta(h_1)\theta(h_2)T_{h_1}T_{h_2} - \sigma(h_1,h_2)\theta(h_1h_2)T_{h_1h_2} \\ &= \big(\theta(h_1)\theta(h_2)\tau(h_1,h_2) - \sigma(h_1,h_2)\theta(h_1h_2)\big)T_{h_1h_2} \\ &= 0 \end{aligned}$$

$$\begin{aligned} f'(W_1 - 1) &= f'(W_1) - g(1) \\ &= \theta(1)T_1 - 1 \\ &= T_1 - 1 \\ &= 0 \end{aligned}$$

$$\begin{aligned} f'(YW_h - \chi(h)W_hY) &= f'(Y)f'(W_h) - \chi(h)f'(W_h)f'(Y) \\ &= \theta(h)XT_h - \chi(h)\theta(h)T_hX \\ &= \theta(h)\big(XT_h - \chi(h)T_hX\big) \\ &= 0 \end{aligned}$$

$$\begin{aligned} f'(Y^d - aW_{g^d}) &= f'(Y)^d - af'(W_{g^d}) \\ &= X^d - a\theta(g^d)T_{g^d} \\ &= \big(b - a\theta(g^d)\big)T_{g^d} \\ &= 0 \end{aligned}$$

Portanto $\mathcal{I}_{\sigma,a}(\mathbb{G}) \subset \ker f'$. Pelo Corolário 1.15, existe um morfismo de $A(\mathbb{G})$-comódulo álgebras entre $A_{\sigma,a}(\mathbb{G})$ e $A_{\tau,b}(\mathbb{G})$. Como ambos são objetos $A(\mathbb{G})$-Galois, segue que são isomorfos. $\square$

Proposição 2.24. *A álgebra $A_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois se, e somente se, vale a equação:*

$$\boxed{a\sigma(g^d, h) = a\chi(h)^d\sigma(h, g^d), \quad \forall h \in G} \tag{2.4.1}$$

Demonstração. ($\Rightarrow$) Pela Proposição 2.15, o conjunto $\{T_hX^i;\ h \in G, 0 \leq i \leq d-1\}$ é uma base de $A_{\sigma,a}(\mathbb{G})$ sobre $\mathbb{K}$. Para cada $h \in G$ temos:

$$\begin{aligned} a\sigma(g^d, h)T_{g^dh} &= aT_{g^d}T_h \\ &= X^dT_h \\ &= \chi(h)^dT_hX^d \\ &= a\chi(h)^dT_hT_{g^d} \\ &= a\chi(h)^d\sigma(h, g^d)T_{hg^d} \end{aligned}$$

e como g é central em G, temos que $a\sigma(g^d, h) = a\chi(h)^d\sigma(h, g^d)$.

($\Leftarrow$) Pela Proposição 2.15, a álgebra $A_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois se o conjunto:

$$\{T_hX^i;\ h \in G, 0 \leq i \leq d-1\}$$

é uma base sobre $\mathbb{K}$. Para provar este fato, utilizaremos o Teorema C.1 (Lema do Diamante), apresentado no Apêndice C.

Os monômios da forma T_hX^i são exatamente os elementos irredutíveis. Vejamos que com a equação (2.4.1), todas as ambiguidades são resolúveis. São elas:

- $(T_{h_1}T_{h_2}T_{h_3})$: Neste caso, podemos utilizar primeiro a igualdade $T_{h_1}T_{h_2} = \sigma(h_1, h_2)T_{h_1h_2}$, obtendo:

$$\begin{aligned} (T_{h_1}T_{h_2})T_{h_3} &= \sigma(h_1, h_2)T_{h_1h_2}T_{h_3} \\ &= \sigma(h_1, h_2)\sigma(h_1h_2, h_3)T_{h_1h_2h_3} \end{aligned}$$

  ou podemos utilizar primeiro a igualdade $T_{h_2}T_{h_3} = \sigma(h_2, h_3)T_{h_2h_3}$, obtendo:

$$\begin{aligned} T_{h_1}(T_{h_2}T_{h_3}) &= \sigma(h_2, h_3)T_{h_1}T_{h_2h_3} \\ &= \sigma(h_2, h_3)\sigma(h_1, h_2h_3)T_{h_1h_2h_3} \end{aligned}$$

  Como $\sigma \in Z^2(G, \mathbb{K}^*)$, temos que:

$$\sigma(h_1, h_2)\sigma(h_1h_2, h_3) = \sigma(h_2, h_3)\sigma(h_1, h_2h_3)$$

  e portanto a ambiguidade é resolúvel.

- (T_1T_h):

$$\begin{aligned} T_1T_h &= \sigma(1, h)T_{1h} \\ &= \varepsilon(h)T_h \end{aligned}$$

$$\begin{aligned} T_1T_h &= 1T_h \\ &= T_h \end{aligned}$$

  Como $\varepsilon(h) = 1$, $\forall h \in G$, temos:

$$\varepsilon(h)T_h = T_h$$

- (T_hT_1):

$$\begin{aligned} T_hT_1 &= \sigma(h,1)T_{h1} \\ &= \varepsilon(h)T_h \end{aligned}$$

$$\begin{aligned} T_hT_1 &= T_h1 \\ &= T_h \end{aligned}$$

Como $\varepsilon(h) = 1$, $\forall h \in G$, temos:

$$\varepsilon(h)T_h = T_h$$

- $(XT_{h_1}T_{h_2})$:

$$\begin{aligned} (XT_{h_1})T_{h_2} &= \chi(h_1)T_{h_1}XT_{h_2} \\ &= \chi(h_1)\chi(h_2)T_{h_1}T_{h_2}X \\ &= \chi(h_1)\chi(h_2)\sigma(h_1,h_2)T_{h_1h_2}X \end{aligned}$$

$$\begin{aligned} X(T_{h_1}T_{h_2}) &= \sigma(h_1,h_2)XT_{h_1h_2} \\ &= \chi(h_1h_2)\sigma(h_1,h_2)T_{h_1h_2}X \end{aligned}$$

Como $\chi\colon G \to \mathbb{K}^*$ é morfismo de grupos, temos:

$$\chi(h_1)\chi(h_2)\sigma(h_1,h_2)T_{h_1h_2}X = \chi(h_1h_2)\sigma(h_1,h_2)T_{h_1h_2}X$$

- (XT_1):

$$XT_1 = \chi(1)T_1X$$

$$\begin{aligned} XT_1 &= X1 \\ &= X \end{aligned}$$

Como $\chi(1) = 1$ e $T_1 = 1$, temos:

$$\chi(1)T_1X = X$$

- (X^dT_h):

$$\begin{aligned} (X^d)T_h &= aT_{g^d}T_h \\ &= a\sigma(g^d,h)T_{g^dh} \end{aligned}$$

$$\begin{aligned} X^dT_h &= \chi(h)^dT_hX^d \\ &= a\chi(h)^dT_hT_{g^d} \\ &= a\chi(h)^d\sigma(h,g^d)T_{hg^d} \end{aligned}$$

Como $g \in G$ é central e $a\sigma(g^d,h) = a\chi(h)^d\sigma(h,g^d), \quad \forall h \in G$, temos:

$$a\sigma(g^d,h)T_{g^dh} = a\chi(h)^d\sigma(h,g^d)T_{hg^d}$$

- (X^{d+1}):

$$\begin{aligned} X\,X^d &= aXT_{g^d} \\ &= a\chi(g^d)T_{g^d}X \end{aligned}$$

$$X^dX = aT_{g^d}X$$

Como $d = o(\chi(g))$ e χ é morfismo de grupos, temos:

$$\begin{aligned} a\chi(g^d)T_{g^d}X &= a\chi(g)^dT_{g^d}X \\ &= aT_{g^d}X \end{aligned}$$

Portanto todas as ambiguidades são resolúveis.

Pelo Lema do Diamante, temos que $\{T_hX^i;\ h \in G, 0 \leq i \leq d-1\}$ é base de $A_{\sigma,a}(\mathbb{G})$. Pela Proposição 2.15, $A_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois. □

2.5 Descrição dos objetos $A(\mathbb{G})$-Galois com $\mathbb{G}$ do tipo I ao tipo V

Nesta seção demonstraremos o Teorema 2.11, exceto para conjunto de dados de grupo do tipo VI, dividindo a demonstração em 5 proposições.

Proposição 2.25. *Seja $\mathbb{G} = (G, g, \chi)$ um conjunto de dados do tipo I. Então temos:*

$$H^2(G, \mathbb{K}^*) \times \mathbb{K} \cong Gal\big(A(\mathbb{G})\big)$$

Demonstração. Para qualquer $\sigma \in Z^2(G, \mathbb{K}^*)$ e $a \in \mathbb{K}$ a equação (2.4.1) é satisfeita. Pela Proposição 2.24, $A_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois.

Considere a função:

$$\begin{aligned} Z^2(G, \mathbb{K}^*) \times \mathbb{K} &\longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big) \\ (\sigma, a) &\longmapsto [A_{\sigma,a}(\mathbb{G})] \end{aligned}$$

Como $g^d = 1$, pela Proposição 2.23, temos que:

$$[A_{\sigma,a}(\mathbb{G})] = [A_{\tau,b}(\mathbb{G})] \iff \sigma = \partial(\theta)\tau \text{ e } b = a$$

para algum $\theta\colon G \to \mathbb{K}^*$ com $\theta(1) = 1$.

Logo a função acima induz uma função injetora:

$$\begin{aligned} H^2(G, \mathbb{K}^*) \times \mathbb{K} &\longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big) \\ (\bar{\sigma}, a) &\longmapsto [A_{\sigma,a}(\mathbb{G})] \end{aligned}$$

Pelo Teorema 2.21, a função acima é sobrejetora e portanto é bijetora. □

Proposição 2.26. *Seja $\mathbb{G} = (G, g, \chi)$ um conjunto de dados do tipo II. Então temos:*

$$H^2(G, \mathbb{K}^*) \cong Gal\big(A(\mathbb{G})\big)$$

Demonstração. Para qualquer $\sigma \in Z^2(G, \mathbb{K}^*)$, tomando $a = 0$, a equação (2.4.1) é satisfeita. Pela Proposição 2.24, $A_{\sigma,0}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois.

Considere a função:

$$\begin{aligned} Z^2(G, \mathbb{K}^*) &\longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big) \\ \sigma &\longmapsto [A_{\sigma,0}(\mathbb{G})] \end{aligned}$$

Pela Proposição 2.23, temos que:

$$[A_{\sigma,0}(\mathbb{G})] = [A_{\tau,0}(\mathbb{G})] \iff \sigma = \partial(\theta)\tau$$

para algum $\theta\colon G \to \mathbb{K}^*$ com $\theta(1) = 1$.

Logo a função acima induz uma função injetora:

$$\begin{aligned} H^2(G,\mathbb{K}^*) &\longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big) \\ \bar{\sigma} &\longmapsto [A_{\sigma,0}(\mathbb{G})] \end{aligned}$$

Pelo Teorema 2.21, dado T um objeto $A(\mathbb{G})$-Galois, existem $\sigma \in Z^2(G,\mathbb{K}^*)$ e $a \in \mathbb{K}$ tais que $T \cong A_{\sigma,a}(\mathbb{G})$. Mas como $\chi^d \neq 1$ e $g^d = 1$, a equação (2.4.1) é satisfeita somente se $a = 0$. Então a função acima é sobrejetora e portanto, bijetora. □

Proposição 2.27. *Seja $\mathbb{G} = (G, g, \chi)$ um conjunto de dados do tipo III. Então temos:*

$$H^2(G,\mathbb{K}^*) \coprod H^2_{g^d,g^d}(G,\mathbb{K}^*) \cong Gal\big(A(\mathbb{G})\big)$$

Demonstração. Para qualquer $\sigma \in Z^2(G,\mathbb{K}^*)$, tomando $a = 0$, a equação (2.4.1) é satisfeita. Pela Proposição 2.24, $A_{\sigma,0}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois.

Considere a função:

$$\begin{aligned} Z^2(G,\mathbb{K}^*) &\longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big) \\ \sigma &\longmapsto [A_{\sigma,0}(\mathbb{G})] \end{aligned}$$

Pela Proposição 2.23, temos que:

$$[A_{\sigma,0}(\mathbb{G})] = [A_{\tau,b}(\mathbb{G})] \iff \sigma = \partial(\theta)\tau \text{ e } b = 0$$

para algum $\theta\colon G \to \mathbb{K}^*$ com $\theta(1) = 1$.

Logo a função acima induz uma função injetora:

$$\begin{aligned} H^2(G,\mathbb{K}^*) &\longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big) \\ \bar{\sigma} &\longmapsto [A_{\sigma,0}(\mathbb{G})] \end{aligned}$$

Para $a = 1$, como $\chi^d = 1$, tomando qualquer $\sigma \in Z^2_{g^d}(G,\mathbb{K}^*)$, a equação (2.4.1) é satisfeita. Pela Proposição 2.24, $A_{\sigma,1}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois.

Considere a função:

$$\begin{aligned} Z^2_{g^d}(G,\mathbb{K}^*) &\longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big) \\ \sigma &\longmapsto [A_{\sigma,1}(\mathbb{G})] \end{aligned}$$

Pela Proposição 2.23, temos que:

$$[A_{\sigma,1}(\mathbb{G})] = [A_{\tau,1}(\mathbb{G})] \iff \sigma = \partial(\theta)\tau \text{ e } \theta(g^d) = 1$$

para algum $\theta\colon G \to \mathbb{K}^*$ com $\theta(1) = 1$.

Logo a função acima induz uma função injetora:

$$\begin{aligned} H^2_{g^d,g^d}(G,\mathbb{K}^*) &\longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big) \\ \bar{\sigma} &\longmapsto [A_{\sigma,1}(\mathbb{G})] \end{aligned}$$

Pelo Teorema 2.21, dado T um objeto $A(\mathbb{G})$-Galois, existem $\sigma \in Z^2(G,\mathbb{K}^*)$ e $a \in \mathbb{K}$ tais que $T \cong A_{\sigma,a}(\mathbb{G})$. Como $\chi^d = 1$, se $a \neq 0$, a equação (2.4.1) é satisfeita somente se $\sigma \in Z^2_{g^d}(G,\mathbb{K}^*)$.

Neste caso, tomando $\theta\colon G \to \mathbb{K}^*$ com $\theta(1) = 1$ e $\theta(g^d) = a$, pela Proposição 2.23, temos que $[A_{\sigma,a}(\mathbb{G})] = [A_{\partial(\theta)\sigma,1}(\mathbb{G})]$. Então a função:

$$H^2(G,\mathbb{K}^*) \coprod H^2_{g^d,g^d}(G,\mathbb{K}^*) \longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big)$$
$$\bar{\sigma} \longmapsto \begin{cases} [A_{\sigma,0}(\mathbb{G})]\,, & \text{se } \sigma \in H^2(G,\mathbb{K}^*) \\ [A_{\sigma,1}(\mathbb{G})]\,, & \text{se } \sigma \in H^2_{g^d,g^d}(G,\mathbb{K}^*) \end{cases}$$

é sobrejetora e portanto, bijetora. □

Proposição 2.28. *Seja $\mathbb{G} = (G, g, \chi)$ um conjunto de dados do tipo IV. Então temos:*

$$H^2(G,\mathbb{K}^*) \cong Gal\big(A(\mathbb{G})\big)$$

Demonstração. Para qualquer $\sigma \in Z^2(G,\mathbb{K}^*)$, tomando $a = 0$, a equação (2.4.1) é satisfeita. Pela Proposição 2.24, $A_{\sigma,0}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois.

Considere a função:

$$Z^2(G,\mathbb{K}^*) \longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big)$$
$$\sigma \longmapsto [A_{\sigma,0}(\mathbb{G})]$$

Pela Proposição 2.23, temos que:

$$[A_{\sigma,0}(\mathbb{G})] = [A_{\tau,0}(\mathbb{G})] \iff \sigma = \partial(\theta)\tau$$

para algum $\theta\colon G \to \mathbb{K}^*$ com $\theta(1) = 1$.

Logo a função acima induz uma função injetora:

$$H^2(G,\mathbb{K}^*) \longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big)$$
$$\bar{\sigma} \longmapsto [A_{\sigma,0}(\mathbb{G})]$$

Pelo Teorema 2.21, dado T um objeto $A(\mathbb{G})$-Galois, existem $\sigma \in Z^2(G,\mathbb{K}^*)$ e $a \in \mathbb{K}$ tais que $T \cong A_{\sigma,a}(\mathbb{G})$. Mas como $\chi^d \neq 1$, $g^d \neq 1$ e não existe $\sigma \in Z^2(G,\mathbb{K}^*)$ tal que $\chi^d(h)\sigma(h,g^d) = \sigma(g^d,h)$, a equação (2.4.1) é satisfeita somente se $a = 0$. Então a função acima é sobrejetora e portanto, bijetora. □

Proposição 2.29. *Seja $\mathbb{G} = (G, g, \chi)$ um conjunto de dados do tipo V. Então temos:*

$$H^2(G,\mathbb{K}^*) \coprod H^2_{g^d,g^d}(G,\mathbb{K}^*) \cong Gal\big(A(\mathbb{G})\big)$$

Demonstração. Para qualquer $\sigma \in Z^2(G,\mathbb{K}^*)$, tomando $a = 0$, a equação (2.4.1) é satisfeita. Pela Proposição 2.24, $A_{\sigma,0}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois.

Considere a função:

$$Z^2(G,\mathbb{K}^*) \longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big)$$
$$\sigma \longmapsto [A_{\sigma,0}(\mathbb{G})]$$

Pela Proposição 2.23, temos que:

$$[A_{\sigma,0}(\mathbb{G})] = [A_{\tau,b}(\mathbb{G})] \iff \sigma = \partial(\theta)\tau \text{ e } b = 0$$

para algum $\theta\colon G \to \mathbb{K}^*$ com $\theta(1) = 1$.

Logo a função acima induz uma função injetora:

$$H^2(G,\mathbb{K}^*) \longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big)$$
$$\bar{\sigma} \longmapsto [A_{\sigma,0}(\mathbb{G})]$$

Seja $\nu \in Z^2(G, \mathbb{K}^*)$ tal que:

$$\chi^d(h)\nu(h, g^d) = \nu(g^d, h),\ \forall h \in G$$

Para $a = 1$, tomando qualquer $\sigma \in Z^2_{g^d}(G, \mathbb{K}^*)$, temos que:

$$\chi^d(h)\nu(h, g^d)\sigma(h, g^d) = \nu(g^d, h)\sigma(g^d, h),\ \forall h \in G$$

Pela Proposição 2.24, $A_{\nu\sigma,1}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois.

Considere a função:

$$\begin{aligned} Z^2_{g^d}(G, \mathbb{K}^*) &\longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big) \\ \sigma &\longmapsto [A_{\nu\sigma,1}(\mathbb{G})] \end{aligned}$$

Pela Proposição 2.23, temos que:

$$[A_{\nu\sigma,1}(\mathbb{G})] = [A_{\nu\tau,1}(\mathbb{G})] \iff \sigma = \partial(\theta)\tau \text{ e } \theta(g^d) = 1$$

para algum $\theta\colon G \to \mathbb{K}^*$ com $\theta(1) = 1$.

Logo a função acima induz uma função injetora:

$$\begin{aligned} H^2_{g^d,g^d}(G, \mathbb{K}^*) &\longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big) \\ \bar{\sigma} &\longmapsto [A_{\nu\sigma,1}(\mathbb{G})] \end{aligned}$$

Pelo Teorema 2.21, dado T um objeto $A(\mathbb{G})$-Galois, existem $\sigma \in Z^2(G, \mathbb{K}^*)$ e $a \in \mathbb{K}$ tais que $T \cong A_{\sigma,a}(\mathbb{G})$. Se $a \neq 0$, a equação (2.4.1) é satisfeita somente se $\sigma \in Z^2(G, \mathbb{K}^*)$ é tal que:

$$\chi^d(h)\sigma(h, g^d) = \sigma(g^d, h),\ \forall h \in G$$

Neste caso, $\nu^{-1}\sigma \in Z^2_{g^d}(G, \mathbb{K}^*)$ e tomando $\theta\colon G \to \mathbb{K}^*$ com $\theta(1) = 1$ e $\theta(g^d) = a$, pela Proposição 2.23, temos que $[A_{\sigma,a}(\mathbb{G})] = [A_{\nu\partial(\theta)\nu^{-1}\sigma,1}(\mathbb{G})]$. Então a função:

$$\begin{aligned} H^2(G, \mathbb{K}^*) \coprod H^2_{g^d,g^d}(G, \mathbb{K}^*) &\longrightarrow \mathrm{Gal}\big(A(\mathbb{G})\big) \\ \bar{\sigma} &\longmapsto \begin{cases} [A_{\sigma,0}(\mathbb{G})]\,, & \text{se } \sigma \in H^2(G, \mathbb{K}^*) \\ [A_{\nu\sigma,1}(\mathbb{G})]\,, & \text{se } \sigma \in H^2_{g^d,g^d}(G, \mathbb{K}^*) \end{cases} \end{aligned}$$

é sobrejetora e portanto, bijetora. □

3. DESCRIÇÃO DOS OBJETOS $A(\mathbb{G})$-BIGALOIS

No capítulo anterior, descrevemos os objetos $A(\mathbb{G})$-Galois para conjuntos de dados de grupo do tipo I ao tipo V. A fim de demonstrar o Teorema 2.11 para conjuntos de dados de grupo do tipo VI, precisamos estudar os objetos $A(\mathbb{G})$-biGalois. Neste capítulo apresentaremos alguns resultados necessários para a demonstração do seguinte teorema:

Teorema 3.1. *Seja $\mathbb{G} = (G, g, \chi, \mu)$ um conjunto de dados de grupo. Então de acordo com o tipo de $\mathbb{G}$, temos o seguinte isomorfismo de grupos para $BiGal(A(\mathbb{G}))$:*

- ***Tipo I:*** $BiGal(A(\mathbb{G})) \cong \Gamma(\mathbb{G}) \ltimes \mathbb{K}$
- ***Tipo II, III, IV, V e VI:*** $BiGal(A(\mathbb{G})) \cong \Gamma(\mathbb{G})$

No teorema, $\Gamma(\mathbb{G})$ é um subgrupo de $\mathrm{Aut}_g(G) \ltimes H^2_{1,g}(G, \mathbb{K}^*)$ que será construído ao longo deste capítulo.

Comecemos fazendo a seguinte observação:

Observação 3.2. *Sejam $\mathbb{G}$ um conjunto de dados de grupo, que pode ser do tipo I ao tipo V, $\sigma \in Z^2(G, \mathbb{K}^*)$ e $a \in \mathbb{K}$ tais que $A_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois à direita. Então a estrutura análoga à coação à direita de $A(\mathbb{G})$ sobre $A_{\sigma,a}(\mathbb{G})$ dada por:*

$$\begin{aligned} \beta\colon A_{\sigma,a}(\mathbb{G}) &\longrightarrow A(\mathbb{G}) \otimes A_{\sigma,a}(\mathbb{G}) \\ X &\longmapsto 1 \otimes X + x \otimes T_g \\ T_h &\longmapsto h \otimes T_h,\ \forall h \in G \end{aligned}$$

pode não dar estrutura de $A(\mathbb{G})$-$A(\mathbb{G})$-bicomódulo álgebra para $A_{\sigma,a}(\mathbb{G})$.

De fato, precisamos que $\beta(XT_h) = \beta(\chi(h)T_hX)$, $\forall h \in G$. Mas:

$$\begin{aligned} \beta(XT_h) &= (1 \otimes X + x \otimes T_g)(h \otimes T_h) \\ &= h \otimes XT_h + xh \otimes T_gT_h \\ &= \chi(h)\big(h \otimes T_hX + \sigma(g,h)hx \otimes T_{gh}\big) \end{aligned}$$

$$\begin{aligned} \beta(\chi(h)T_hX) &= \chi(h)\big((h \otimes T_h)(1 \otimes X + x \otimes T_g)\big) \\ &= \chi(h)\big(h \otimes T_hX + hx \otimes T_hT_g\big) \\ &= \chi(h)\big(h \otimes T_hX + \sigma(h,g)hx \otimes T_{gh}\big) \end{aligned}$$

e nada garante que $\sigma(g,h) = \sigma(h,g)$, $\forall h \in G$.

Existem pelo menos duas formas de resolver este problema:

1) Trocar a estrutura de $A(\mathbb{G})$-comódulo à esquerda por:

$$\begin{aligned} \beta_u\colon A_{\sigma,a}(\mathbb{G}) &\longrightarrow A(\mathbb{G}) \otimes A_{\sigma,a}(\mathbb{G}) \\ X &\longmapsto 1 \otimes X + x \otimes T_g \\ T_h &\longmapsto u(h) \otimes T_h,\ \forall h \in G \end{aligned}$$

   para algum $u\colon G \to G$ apropriado.

2) Escolher um segundo conjunto de dados de grupo $\mathbb{G}' = (G, g, \chi', \mu)$, de modo que $A_{\sigma,a}(\mathbb{G})$ seja $A(\mathbb{G}')$-$A(\mathbb{G})$-bicomódulo álgebra com coação à esquerda dada por:

$$\begin{aligned} \beta\colon A_{\sigma,a}(\mathbb{G}) &\longrightarrow A(\mathbb{G}') \otimes A_{\sigma,a}(\mathbb{G}) \\ X &\longmapsto 1 \otimes X + x \otimes T_g \\ T_h &\longmapsto h \otimes T_h,\ \forall h \in G \end{aligned}$$

Estudando apenas o primeiro caso é possível resolver o Teorema 3.1 para conjuntos de dados do tipo I e II. Para os demais, é necessário estudar ambos os casos, como veremos a seguir.

3.1 Os objetos $A(\mathbb{G})$-biGalois $A^u_{\sigma,a}(\mathbb{G})$

Nesta seção apresentaremos a álgebra $A^u_{\sigma,a}(\mathbb{G})$ e como ela está relacionada com a estrutura de grupo de $\mathrm{BiGal}(A(\mathbb{G}))$.

Proposição 3.3. *Sejam $\mathbb{G} = (G, g, \chi)$ um conjunto de dados de grupo, $\sigma \in Z^2(G, \mathbb{K}^*)$ e $a \in \mathbb{K}$ tal que $a = 0$ se $\mathbb{G}$ não é do tipo I. Então $A_{\sigma,a}(\mathbb{G})$ é um objeto $A(\mathbb{G})$-Galois à direita e, temos que $A_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois com coação à esquerda dada por:*

$$\begin{aligned} \beta_u\colon A_{\sigma,a}(\mathbb{G}) &\longrightarrow A(\mathbb{G}) \otimes A_{\sigma,a}(\mathbb{G}) \\ X &\longmapsto 1 \otimes X + x \otimes T_g \\ T_h &\longmapsto u(h) \otimes T_h,\ \forall h \in G \end{aligned}$$

com $u\colon G \to G$ se, e somente se, $u \in Aut_g(G)$ e:

$$\chi \circ u(h) = \sigma(g,h)^{-1}\sigma(h,g)\chi(h),\ \forall h \in G$$

Denotaremos este objeto $A(\mathbb{G})$-biGalois por $A^u_{\sigma,a}(\mathbb{G})$.

Demonstração. ($\Rightarrow$) Como β_u está bem definido, temos que $\beta_u(T_{h_1}T_{h_2}) = \beta_u(\sigma(h_1,h_2)T_{h_1h_2})$, $\forall h_1, h_2 \in G$. Mas:

$$\begin{aligned} \beta_u(T_{h_1}T_{h_2}) &= (u(h_1) \otimes T_{h_1})(u(h_2) \otimes T_{h_2}) \\ &= u(h_1)u(h_2) \otimes T_{h_1}T_{h_2} \\ &= \sigma(h_1,h_2)u(h_1)u(h_2) \otimes T_{h_1h_2} \end{aligned}$$

$$\begin{aligned} \beta_u(\sigma(h_1,h_2)T_{h_1h_2}) &= \sigma(h_1,h_2)\beta_u(T_{h_1h_2}) \\ &= \sigma(h_1,h_2)u(h_1h_2) \otimes T_{h_1h_2} \end{aligned}$$

Além disso, temos que $\beta_u(T_1) = \beta_u(1)$. Mas:

$$\beta_u(T_1) = u(1) \otimes T_1$$

$$\begin{aligned} \beta_u(1) &= 1 \otimes 1 \\ &= 1 \otimes T_1 \end{aligned}$$

Logo $u(h_1h_2) = u(h_1)u(h_2)$, $\forall h_1, h_2 \in G$ e $u(1) = 1$. Portanto u é morfismo de grupos.

Como β_u é coação, temos que $(A(\mathbb{G}) \otimes \beta_u) \circ \beta_u = (\Delta_{A(\mathbb{G})} \otimes A_{\sigma,a}(\mathbb{G})) \circ \beta_u$. Calculando em X, temos:

$$\begin{aligned} (A(\mathbb{G}) \otimes \beta_u) \circ \beta_u(X) &= (A(\mathbb{G}) \otimes \beta_u)(1 \otimes X + x \otimes T_g) \\ &= 1 \otimes (1 \otimes X + x \otimes T_g) + x \otimes u(g) \otimes T_g) \\ &= 1 \otimes 1 \otimes X + 1 \otimes x \otimes T_g + x \otimes u(g) \otimes T_g \end{aligned}$$

$$
\begin{aligned}
(\Delta_{A(\mathbb{G})} \otimes A_{\sigma,a}(\mathbb{G})) \circ \beta_u(X) &= (\Delta \otimes A_{\sigma,a}(\mathbb{G}))(1 \otimes X + x \otimes T_g) \\
&= 1 \otimes 1 \otimes X + (1 \otimes x + x \otimes g) \otimes T_g \\
&= 1 \otimes 1 \otimes X + 1 \otimes x \otimes T_g + x \otimes g \otimes T_g
\end{aligned}
$$

Portanto $u(g) = g$.

Como κ_l é isomorfismo e para cada $h \in G$ vale que:

$$
\begin{aligned}
\kappa_l(\sigma(h,h^{-1})^{-1} T_h \otimes T_{h^{-1}}) &= \sigma(h,h^{-1}) \beta_u(T_h) T_{h^{-1}} \\
&= \sigma(h,h^{-1}) u(h) \otimes T_h T_{h^{-1}} \\
&= u(h) \otimes 1
\end{aligned}
$$

temos que u é monomorfismo. Como G é finito, segue que $u \in \mathrm{Aut}_g(G)$.

Para cada $h \in G$ temos:

$$
\begin{aligned}
\beta_u(XT_h) &= (1 \otimes X + x \otimes T_g)(u(h) \otimes T_h) \\
&= u(h) \otimes XT_h + xu(h) \otimes T_g T_h \\
&= \chi(h)u(h) \otimes T_h X + \chi(u(h))\sigma(g,h)u(h)x \otimes T_{gh}
\end{aligned}
$$

$$
\begin{aligned}
\beta_u(\chi(h)T_h X) &= \chi(h)\big((u(h) \otimes T_h)(1 \otimes X + x \otimes T_g)\big) \\
&= \chi(h)\big(u(h) \otimes T_h X + hx \otimes T_h T_g\big) \\
&= \chi(h)\big(u(h) \otimes T_h X + \sigma(h,g)u(h)x \otimes T_{gh}\big) \\
&= \chi(h)u(h) \otimes T_h X + \chi(h)\sigma(h,g)u(h)x \otimes T_{gh}
\end{aligned}
$$

Portanto $\chi(u(h))\sigma(g,h) = \chi(h)\sigma(h,g)$, $\forall h \in G$.

($\Leftarrow$) Vejamos que $\mathcal{V}(\mathbb{G})$ é $A(\mathbb{G})$-comódulo à esquerda com:

$$
\begin{aligned}
f\colon \mathcal{V}(\mathbb{G}) &\longrightarrow A(\mathbb{G}) \otimes \mathcal{V}(\mathbb{G}) \\
Y &\longmapsto 1 \otimes Y + x \otimes W_g \\
W_h &\longmapsto u(h) \otimes W_h, \ \forall h \in G
\end{aligned}
$$

De fato, temos:

$$
\begin{aligned}
(A(\mathbb{G}) \otimes f) \circ f(Y) &= (A(\mathbb{G}) \otimes f)(1 \otimes Y + x \otimes W_g) \\
&= 1 \otimes (1 \otimes Y + x \otimes W_g) + x \otimes u(g) \otimes W_g \\
&= 1 \otimes 1 \otimes Y + 1 \otimes x \otimes W_g + x \otimes g \otimes W_g \\
&= (\Delta_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G}))(1 \otimes Y) + (\Delta_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G}))(x \otimes W_g) \\
&= (\Delta_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G})) \circ f(Y)
\end{aligned}
$$

e para cada $h \in G$ temos:

$$
\begin{aligned}
(A(\mathbb{G}) \otimes f) \circ f(W_h) &= (A(\mathbb{G}) \otimes f)(u(h) \otimes W_h) \\
&= u(h) \otimes u(h) \otimes W_h \\
&= (\Delta \otimes \mathcal{V}(\mathbb{G}))(u(h) \otimes W_h) \\
&= (\Delta_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G})) \circ f(W_h)
\end{aligned}
$$

Além disso, como $\varepsilon_{A(\mathbb{G})}(h) = 1, \forall h \in G$ e $\varepsilon_{A(\mathbb{G})}(x) = 0$, temos:

$$
\begin{aligned}
(\varepsilon_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G})) \circ f(Y) &= (\varepsilon_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G}))(1 \otimes Y + x \otimes W_g) \\
&= \varepsilon_{A(\mathbb{G})}(1) \otimes Y + \varepsilon_{A(\mathbb{G})}(x) \otimes W_g \\
&= 1 \otimes Y
\end{aligned}
$$

e para cada $h \in G$ temos:

$$\begin{aligned}(\varepsilon_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G})) \circ f(W_h) &= (\varepsilon_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G}))(u(h) \otimes W_h) \\ &= \varepsilon_{A(\mathbb{G})}(u(h)) \otimes W_h \\ &= 1 \otimes W_h\end{aligned}$$

Portanto $\mathcal{V}(\mathbb{G})$ é $A(\mathbb{G})$-comódulo com a estrutura acima.

Pela Teorema 1.10, $\mathcal{L}(\mathbb{G})$ é $A(\mathbb{G})$-comódulo álgebra com coação dada por:

$$\begin{aligned} f' \colon \mathcal{L}(\mathbb{G}) &\longrightarrow A(\mathbb{G}) \otimes \mathcal{L}(\mathbb{G}) \\ Y &\longmapsto 1 \otimes Y + x \otimes W_g \\ W_h &\longmapsto u(h) \otimes W_h,\ \forall h \in G\end{aligned}$$

Vejamos que $f'(\mathcal{I}_{\sigma,a}(\mathbb{G})) \subset A(\mathbb{G}) \otimes \mathcal{I}_{\sigma,a}(\mathbb{G})$. De fato, nos geradores de $\mathcal{I}_{\sigma,a}(\mathbb{G})$, como $u \in \mathrm{Aut}_g(G)$, temos:

$$\begin{aligned} f'(W_{h_1}W_{h_2} - \sigma(h_1,h_2)W_{h_1h_2}) &= u(h_1)u(h_2) \otimes W_{h_1}W_{h_2} - \sigma(h_1,h_2)u(h_1h_2) \otimes W_{h_1h_2} \\ &= u(h_1h_2) \otimes W_{h_1}W_{h_2} - \sigma(h_1,h_2)u(h_1h_2) \otimes W_{h_1h_2} \\ &= u(h_1h_2) \otimes (W_{h_1}W_{h_2} - \sigma(h_1,h_2)W_{h_1h_2})\end{aligned}$$

e

$$\begin{aligned} f'(W_1 - 1) &= u(1) \otimes W_1 - 1 \otimes 1 \\ &= 1 \otimes W_1 - 1 \otimes 1 \\ &= 1 \otimes (W_1 - 1)\end{aligned}$$

Como $\chi \circ u(h) = \sigma(g,h)^{-1}\sigma(h,g)\chi(h)$, então:

$$\begin{aligned} f'(YW_h - \chi(h)W_hY) &= (1 \otimes Y + x \otimes W_g)(u(h) \otimes W_h) - \chi(h)(u(h) \otimes W_h)(1 \otimes Y + x \otimes W_g) \\ &= u(h) \otimes YW_h + xu(h) \otimes W_gW_h - \chi(h)u(h) \otimes W_hY \\ &\quad - \chi(h)u(h)x \otimes W_hW_g \\ &= u(h) \otimes (YW_h - \chi(h)W_hY) + \chi(u(h))xu(h) \otimes W_gW_h \\ &\quad - \chi(h)u(h)x \otimes W_hW_g \\ &= u(h) \otimes (YW_h - \chi(h)W_hY) + \sigma(g,h)^{-1}\sigma(h,g)\chi(h)xu(h) \otimes W_gW_h \\ &\quad - \chi(h)u(h)x \otimes W_hW_g \\ &= u(h) \otimes (YW_h - \chi(h)W_hY) + \sigma(g,h)^{-1}\sigma(h,g)\chi(h)xu(h) \otimes W_gW_h \\ &\quad - \sigma(h,g)\chi(h)xu(h) \otimes W_{gh} + \sigma(h,g)\chi(h)xu(h) \otimes W_{gh} \\ &\quad - \chi(h)u(h)x \otimes W_hW_g \\ &= u(h) \otimes (YW_h - \chi(h)W_hY) \\ &\quad + \sigma(g,h)^{-1}\sigma(h,g)\chi(h)xu(h) \otimes (W_gW_h - \sigma(g,h)W_{gh}) \\ &\quad - \chi(h)u(h)x \otimes (W_hW_g - \sigma(h,g)W_{gh})\end{aligned}$$

Como $a = 0$ se $\mathbb{G}$ não é do tipo I, $g^d = 1$ quando $\mathbb{G}$ é do tipo I, $\pi \colon \mathcal{L}(\mathbb{G}) \to A_{\sigma,a}(\mathbb{G})$ é morfismo de álgebras e $\ker \pi = \mathcal{I}_{\sigma,a}(\mathbb{G})$, temos que:

$$\begin{aligned} (A(\mathbb{G}) \otimes \pi) \circ f'(Y^d - aW_{g^d}) &= (A(\mathbb{G}) \otimes \pi)\big((1 \otimes Y + x \otimes W_g)^d - au(g^d) \otimes W_{g^d}\big) \\ &= (1 \otimes X + x \otimes T_g)^d - ag^d \otimes T_{g^d} \\ &\overset{\text{Corolário A.8}}{=} 1 \otimes X^d + x^d \otimes (T_g)^d - ag^d \otimes T_{g^d} \\ &= a1 \otimes T_{g^d} - ag^d \otimes T_{g^d} \\ &= a(1 - g^d) \otimes T_{g^d} \\ &= 0\end{aligned}$$

implica $f'(Y^d - aW_{g^d}) \in A(\mathbb{G}) \otimes \mathcal{I}_{\sigma,a}(\mathbb{G})$.

Pelo Corolário 1.14, $A_{\sigma,a}(\mathbb{G})$ é $A(\mathbb{G})$-comódulo álgebra com coação dada por:

$$\begin{aligned}\beta_u \colon A_{\sigma,a}(\mathbb{G}) &\longrightarrow A(\mathbb{G}) \otimes A_{\sigma,a}(\mathbb{G})\\ X &\longmapsto 1 \otimes X + x \otimes T_g\\ T_h &\longmapsto u(h) \otimes T_h,\ \forall h \in G\end{aligned}$$

Vejamos que $A_{\sigma,a}(\mathbb{G})$ é $A(\mathbb{G})$-bicomódulo. De fato, como $\{T_hX^i;\, h \in G, 0 \leq i \leq d-1\}$ é base linear de $A_{\sigma,a}(\mathbb{G})$, precisamos verificar apenas para os elementos da base. Sejam $h \in G$ e $0 \leq i \leq d-1$. Como ρ e β são morfismos de álgebras, temos:

$$\begin{aligned}(A(\mathbb{G}) \otimes \rho) \circ \beta_u(T_hX^i) &= (A(\mathbb{G}) \otimes \rho)\big((u(h) \otimes T_h)(1 \otimes X + x \otimes T_g)^i\big)\\ &= (u(h) \otimes T_h \otimes h)(1 \otimes (1 \otimes x + X \otimes g) + x \otimes T_g \otimes g)^i\\ &= (u(h) \otimes T_h \otimes h)(1 \otimes 1 \otimes x + 1 \otimes X \otimes g + x \otimes T_g \otimes g)^i\\ &= (\beta_u \otimes A(\mathbb{G}))\big((T_h \otimes h)(1 \otimes x + X \otimes g)^i\big)\\ &= (\beta_u \otimes A(\mathbb{G})) \circ \rho(T_hX^i)\end{aligned}$$

Portanto $A_{\sigma,a}(\mathbb{G})$ é $A(\mathbb{G})$-bicomódulo.

Vejamos $A_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Balois, ou seja, que a função:

$$\kappa_l \colon A_{\sigma,a}(\mathbb{G}) \otimes A_{\sigma,a}(\mathbb{G}) \to A(\mathbb{G}) \otimes A_{\sigma,a}(\mathbb{G})$$

é bijetora. De fato, para cada $h \in G$, tomando $k \in G$ tal que $u(k) = h$, temos:

$$\begin{aligned}\kappa_l(T_k \otimes 1) &= \beta_u(T_k)1\\ &= u(k) \otimes T_k\\ &= h \otimes T_k\end{aligned}$$

e pela $A_{\sigma,a}(\mathbb{G})$-linearidade à direita temos:

$$\begin{aligned}\kappa_l(\sigma(k,k^{-1})^{-1}T_k \otimes T_{k^{-1}}) &= \sigma(k,k^{-1})^{-1}\kappa_l(T_k \otimes 1)T_{k^{-1}}\\ &= \sigma(k,k^{-1})^{-1}(h \otimes T_k)T_{k^{-1}}\\ &= \sigma(k,k^{-1})^{-1}\sigma(k,k^{-1})h \otimes T_{kk^{-1}}\\ &= h \otimes 1\end{aligned}$$

Assuma que $hx^t \otimes 1$ está na imagem de κ_l, $\forall h \in G$ e $0 \leq t \leq i-1$.

Seja $\eta_{h,t} \in A_{\sigma,a}(\mathbb{G}) \otimes A_{\sigma,a}(\mathbb{G})$ um elemento tal que $\kappa_l(\eta_{h,t}) = hx^t \otimes 1$. Então:

$$\begin{aligned}
\kappa_l(X^i \eta_{h,0}) &= \kappa_l(\sigma(k,k^{-1})^{-1} X^i T_k \otimes T_{k^{-1}}) \\
&= \sigma(k,k^{-1})^{-1} \beta_u(X^i)\beta_u(T_k)T_{k^{-1}} \\
&= \sigma(k,k^{-1})^{-1} (1 \otimes X + x \otimes T_g)^i (u(k) \otimes T_k) T_{k^{-1}} \\
&= (1 \otimes X + x \otimes T_g)^i (h \otimes 1) \\
&\overset{\text{Proposição A.7}}{=} \sum_{t=0}^{i} \binom{i}{t}_q (x \otimes T_g)^{i-t} (1 \otimes X)^t (h \otimes 1) \\
&= \sum_{t=0}^{i} \binom{i}{t}_q x^{i-t} h \otimes (T_g)^{i-t} X^t \\
&= \sum_{t=0}^{i} \binom{i}{t}_q \chi(h)^{i-t} h x^{i-t} \otimes (T_g)^{i-t} X^t \\
&= \chi(h)^i h x^i \otimes (T_g)^i + \sum_{t=1}^{i} \binom{i}{t}_q \chi(h)^{i-t} h x^{i-t} \otimes (T_g)^{i-t} X^t \\
&= \chi(h)^i h x^i \otimes (T_g)^i + \sum_{t=1}^{i} \binom{i}{t}_q \chi(h)^{i-t} \kappa_l(\eta_{h,i-t}) (T_g)^{i-t} X^t
\end{aligned}$$

Portanto temos que:

$$\kappa_l\Big(\chi(h)^{-i}\Big(X^i\eta_{h,0} - \sum_{t=1}^{i} \binom{i}{t}_q \chi(h)^{i-t} \eta_{h,i-t} (T_g)^{i-t} X^t\Big)(T_g)^{-i}\Big) = hx^i \otimes 1$$

Logo, todos os elementos da forma $hx^i \otimes 1$ estão na imagem de κ_l. Como κ_l é $A_{\sigma,a}(\mathbb{G})$-linear à direita, temos que κ_l é sobrejetora.

Assim, temos que $\dim A_{\sigma,a}(\mathbb{G}) \otimes A_{\sigma,a}(\mathbb{G}) \geq \dim A(\mathbb{G}) \otimes A_{\sigma,a}(\mathbb{G})$. Como $A_{\sigma,a}(\mathbb{G})$ é algebra não-nula, $\dim A_{\sigma,a}(\mathbb{G}) \neq 0$. Portanto $\dim A_{\sigma,a}(\mathbb{G}) \geq \dim A(\mathbb{G})$.

Pelo Lema 2.14, temos que $\dim A_{\sigma,a}(\mathbb{G}) \leq |G|d$ e sabemos que $\dim A(\mathbb{G}) = |G|d$. Logo $\dim A_{\sigma,a}(\mathbb{G}) \otimes A_{\sigma,a}(\mathbb{G}) = \dim A(\mathbb{G}) \otimes A_{\sigma,a}(\mathbb{G})$ e κ_l é isomorfismo, o que implica que $A_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois. □

Proposição 3.4. *Sejam $\sigma, \tau \in Z^2(G, \mathbb{K}^*)$, $a, b \in \mathbb{K}$ e $u, v \in Aut_g(G)$ tais que $A^u_{\sigma,a}(\mathbb{G})$ e $A^v_{\tau,b}(\mathbb{G})$ são objetos $A(\mathbb{G})$-biGalois.*

Então $A^u_{\sigma,a}(\mathbb{G})$ e $A^v_{\tau,b}(\mathbb{G})$ são isomorfos como $A(\mathbb{G})$-bicomódulo álgebras se, e somente se, $u = v$ e existe $\theta\colon G \to \mathbb{K}^*$ com $\theta(1) = \theta(g) = 1$ tal que:

$$\sigma = \partial(\theta)\tau \text{ e } b = a\theta(g^d)$$

Demonstração. ($\Rightarrow$) Como $A^u_{\sigma,a}(\mathbb{G})$ e $A^v_{\tau,b}(\mathbb{G})$ são isomorfos como $A(\mathbb{G})$-bicomódulo álgebras, em particular são isomorfos como $A(\mathbb{G})$-comódulo álgebras à direita e, pela Proposição 2.23, existe $\theta\colon G \to \mathbb{K}^*$ com $\theta(1) = 1$, $\sigma = \partial(\theta)\tau$ e $b = a\theta(g^d)$. Durante a demonstração da Proposição 2.23, vemos que o isomorfismo deve ser dado por:

$$\begin{aligned}
f\colon A^u_{\sigma,a}(\mathbb{G}) &\longrightarrow A^v_{\tau,b}(\mathbb{G}) \\
X &\longmapsto X \\
T_h &\longmapsto \theta(h)T_h,\ \forall h \in G
\end{aligned}$$

Temos que $(A(\mathbb{G}) \otimes f) \circ \beta_u = \beta_v \circ f$. Mas para cada $h \in G$ temos:

$$\begin{aligned}(A(\mathbb{G}) \otimes f) \circ \beta_u(T_h) &= (A(\mathbb{G}) \otimes f)(u(h) \otimes T_h)\\ &= \theta(h)u(h) \otimes T_h\end{aligned}$$

$$\begin{aligned}\beta_v \circ f(T_h) &= \beta_v(\theta(h)T_h)\\ &= \theta(h)v(h) \otimes T_h\end{aligned}$$

Como $\theta(h) \neq 0$, $\forall h \in G$, temos que $u(h) = v(h)$, $\forall h \in G$. Além disso, temos:

$$\begin{aligned}(A(\mathbb{G}) \otimes f) \circ \beta_u(X) &= (A(\mathbb{G}) \otimes f)(1 \otimes X + x \otimes T_g)\\ &= 1 \otimes X + \theta(g)x \otimes T_g\end{aligned}$$

$$\begin{aligned}\beta_v \circ f(X) &= \beta_v(X)\\ &= 1 \otimes X + x \otimes T_g\end{aligned}$$

Portanto $\theta(g) = 1$.

($\Leftarrow$) Pela Proposição 2.23, como existe $\theta\colon G \to \mathbb{K}^*$ com $\theta(1) = 1$, $\sigma = \partial(\theta)\tau$ e $b = a\theta(g^d)$, temos que $A^u_{\sigma,a}(\mathbb{G})$ e $A^v_{\tau,b}(\mathbb{G})$ são isomorfos como $A(\mathbb{G})$-comódulo álgebras à direita, com isomorfismo dado por:

$$\begin{aligned}f\colon A^u_{\sigma,a}(\mathbb{G}) &\longrightarrow A^v_{\tau,b}(\mathbb{G})\\ X &\longmapsto X\\ T_h &\longmapsto \theta(h)T_h,\ \forall h \in G\end{aligned}$$

Precisamos verificar que $(A(\mathbb{G}) \otimes f) \circ \beta_u = \beta_v \circ f$. Como $\{T_hX^i;\ h \in G, 0 \leq i \leq d-1\}$ é base linear de $A^u_{\sigma,a}(\mathbb{G})$, podemos verificar apenas para os elementos da base. Para cada $h \in G$ e $0 \leq i \leq d-1$ temos:

$$\begin{aligned}(A(\mathbb{G}) \otimes f) \circ \beta_u(T_hX^i) &= (A(\mathbb{G}) \otimes f)\big((u(h) \otimes T_h)(1 \otimes X + x \otimes T_g)^i\big)\\ &= (\theta(h)u(h) \otimes T_h)(1 \otimes X + \theta(g)x \otimes T_g)^i\end{aligned}$$

$$\begin{aligned}\beta_v \circ f(T_hX^i) &= \beta_v(\theta(h)T_hX^i)\\ &= \theta(h)(v(h) \otimes T_h)(1 \otimes X + x \otimes T_g)^i\end{aligned}$$

Como $u = v$ e $\theta(g) = 1$, temos que $(A(\mathbb{G}) \otimes f) \circ \beta_u = \beta_v \circ f$ e f é isomorfismo de $A(\mathbb{G})$-bicomódulo álgebras. □

Proposição 3.5. *Sejam $\sigma, \tau \in Z^2(G, \mathbb{K}^*)$, $a, b \in \mathbb{K}$ com $a = b = 0$ se $\mathbb{G}$ não é do tipo I e $u, v \in Aut_g(G)$ tais que $A^u_{\sigma,a}(\mathbb{G})$ e $A^v_{\tau,b}(\mathbb{G})$ são objetos $A(\mathbb{G})$-biGalois. Tome $\omega = (\sigma\circ(v\times v))\tau$ e $c = \tau(g,g)\cdots\tau(g,g^{d-1})a+b$. Então $A^{u\circ v}_{\omega,c}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois e temos um isomorfismo de $A(\mathbb{G})$-bicomódulo álgebras:*

$$A^{u\circ v}_{\omega,c}(\mathbb{G}) \cong A^u_{\sigma,a}(\mathbb{G}) \underset{A(\mathbb{G})}{\square} A^v_{\tau,b}(\mathbb{G})$$

Demonstração. Como $A^u_{\sigma,a}(\mathbb{G})$ e $A^v_{\tau,b}(\mathbb{G})$ são objetos $A(\mathbb{G})$-biGalois, em particular são objetos $A(\mathbb{G})$-Galois à direita e, pela Proposição 2.24, temos que para todo $h \in G$:

$$\begin{aligned}a\sigma(g^d, h) &= a\chi(h)^d\sigma(h, g^d)\\ b\tau(g^d, h) &= b\chi(h)^d\tau(h, g^d)\end{aligned}$$

Se $\mathbb{G}$ não é do tipo I, temos que $a = b = 0$, o que implica que $c = 0$ e, pela Proposição 2.24, $A_{\omega,c}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois à direita.

Se $\mathbb{G}$ é do tipo I, basta verificar que $\omega \in Z^2(G, \mathbb{K}^*)$ que a equação (2.4.1) será satisfeita (pois $g^d = 1$ e $\chi^d = 1$) e pela Proposição 2.24, $A_{\omega,c}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois à direita. De fato, dados $h_1, h_2, h_3 \in G$:

$$\begin{aligned}
\omega(h_1,h_2)\omega(h_1h_2,h_3) &= \big((\sigma\circ(v\times v))\tau\big)(h_1,h_2)\big((\sigma\circ(v\times v))\tau\big)(h_1h_2,h_3)\\
&= \sigma(v(h_1),v(h_2))\tau(h_1,h_2)\sigma(v(h_1h_2),v(h_3))\tau(h_1h_2,h_3)\\
&= \sigma(v(h_1),v(h_2))\sigma(v(h_1)v(h_2),v(h_3))\tau(h_1,h_2)\tau(h_1h_2,h_3)\\
&= \sigma(v(h_2),v(h_3))\sigma(v(h_1),v(h_2)v(h_3))\tau(h_2,h_3)\tau(h_1,h_2h_3)\\
&= \sigma(v(h_2),v(h_3))\sigma(v(h_1),v(h_2h_3))\tau(h_2,h_3)\tau(h_1,h_2h_3)\\
&= \big((\sigma\circ(v\times v))\tau\big)(h_2,h_3)\big((\sigma\circ(v\times v))\tau\big)(h_1,h_2h_3)\\
&= \omega(h_2,h_3)\omega(h_1,h_2h_3)
\end{aligned}$$

e $\omega \in Z^2(G, \mathbb{K}^*)$.

Vejamos que $A^{u\circ v}_{\omega,c}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois. De fato, como $u, v \in \mathrm{Aut}_g(G)$ com:

$$\begin{aligned}
\chi\circ u(h) &= \sigma(g,h)^{-1}\sigma(h,g)\chi(h)\\
\chi\circ v(h) &= \tau(g,h)^{-1}\tau(h,g)\chi(h)
\end{aligned}$$

para todo $h \in G$, temos que $u\circ v \in \mathrm{Aut}_g(G)$ e para todo $h \in G$:

$$\begin{aligned}
\chi\circ(u\circ v)(h) &= \chi\circ u(v(h))\\
&= \sigma(g,v(h))^{-1}\sigma(v(h),g)\chi(v(h))\\
&= \sigma(v(g),v(h))^{-1}\sigma(v(h),v(g))\tau(g,h)^{-1}\tau(h,g)\chi(h)\\
&= \omega(g,h)^{-1}\omega(h,g)\chi(h)
\end{aligned}$$

Pela Proposição 3.3, temos que $A^{u\circ v}_{\omega,c}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois.

Pelo Proposição 3.5, temos que $A^u_{\sigma,a}(\mathbb{G}) \underset{A(\mathbb{G})}{\square} A^v_{\tau,b}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois.

Além disso, temos que:

$$\begin{aligned}
(\rho\otimes A^v_{\tau,b}(\mathbb{G}))(1\otimes X + X\otimes T_g) &= 1\otimes 1\otimes X + 1\otimes x\otimes T_g + X\otimes g\otimes T_g\\
&= 1\otimes 1\otimes X + 1\otimes x\otimes T_g + X\otimes v(g)\otimes T_g\\
&= (A^u_{\sigma,a}(\mathbb{G})\otimes\beta_v)(1\otimes X + X\otimes T_g)
\end{aligned}$$

e para cada $h \in G$:

$$\begin{aligned}
(\rho\otimes A^v_{\tau,b}(\mathbb{G}))(T_{v(h)}\otimes T_h) &= T_{v(h)}\otimes v(h)\otimes T_h\\
&= (A^u_{\sigma,a}(\mathbb{G})\otimes\beta_v)(T_{v(h)}\otimes T_h)
\end{aligned}$$

Logo, $1\otimes X + X\otimes T_g$ e $T_{v(h)}\otimes T_h$ pertencem à $A^u_{\sigma,a}(\mathbb{G}) \underset{A(\mathbb{G})}{\square} A^v_{\tau,b}(\mathbb{G})$.

Considere a função:

$$\begin{aligned}
f\colon \mathcal{V}(\mathbb{G}) &\longrightarrow A^u_{\sigma,a}(\mathbb{G}) \underset{A(\mathbb{G})}{\square} A^v_{\tau,b}(\mathbb{G})\\
Y &\longmapsto 1\otimes X + X\otimes T_g\\
W_h &\longmapsto T_{v(h)}\otimes T_h
\end{aligned}$$

onde $\mathcal{V}(\mathbb{G})$ é $A(\mathbb{G})$-bicomódulo com estrutura à direita dada por:

$$\begin{aligned}
\rho_{\mathcal{V}(\mathbb{G})}\colon \mathcal{V}(\mathbb{G}) &\longrightarrow \mathcal{V}(\mathbb{G})\otimes A(\mathbb{G})\\
Y &\longmapsto 1\otimes x + Y\otimes g\\
W_h &\longmapsto W_h\otimes h
\end{aligned}$$

e estrutura à esquerda dada por:

$$\begin{aligned}\beta_{\mathcal{V}(\mathbb{G})}\colon \mathcal{V}(\mathbb{G}) &\longrightarrow A(\mathbb{G})\otimes \mathcal{V}(\mathbb{G})\\ Y &\longmapsto 1\otimes Y + x\otimes T_g\\ W_h &\longmapsto u\circ v(h)\otimes W_h\end{aligned}$$

Vejamos que f é morfismo de $A(\mathbb{G})$-comódulos à direita:

$$\begin{aligned}(A^u_{\sigma,a}(\mathbb{G})\otimes\rho_v)\circ f(Y) &= (A^u_{\sigma,a}(\mathbb{G})\otimes\rho_v)(1\otimes X + X\otimes T_g)\\ &= 1\otimes 1\otimes x + 1\otimes X\otimes g + X\otimes T_g\otimes g\\ &= (f\otimes A(\mathbb{G}))(1\otimes x + Y\otimes g)\\ &= (f\otimes A(\mathbb{G}))\circ\rho_{\mathcal{V}(\mathbb{G})}(Y)\end{aligned}$$

e para cada $h\in G$:

$$\begin{aligned}(A^u_{\sigma,a}(\mathbb{G})\otimes\rho_v)\circ f(W_h) &= (A^u_{\sigma,a}(\mathbb{G})\otimes\rho_v)(T_{v(h)}\otimes T_h)\\ &= T_{v(h)}\otimes T_h\otimes h\\ &= (f\otimes A(\mathbb{G}))(W_h\otimes h)\\ &= (f\otimes A(\mathbb{G}))\circ\rho_{\mathcal{V}(\mathbb{G})}(W_h)\end{aligned}$$

Vejamos que f é morfismo de $A(\mathbb{G})$-comódulos à esquerda:

$$\begin{aligned}(\beta_u\otimes A^v_{\tau,b}(\mathbb{G}))\circ f(Y) &= (\beta_u\otimes A^v_{\tau,b}(\mathbb{G}))(1\otimes X + X\otimes T_g)\\ &= 1\otimes 1\otimes X + 1\otimes X\otimes T_g + x\otimes T_g\otimes T_g\\ &= 1\otimes 1\otimes X + 1\otimes X\otimes T_g + x\otimes T_{v(g)}\otimes T_g\\ &= (A(\mathbb{G})\otimes f)(1\otimes Y + x\otimes W_g)\\ &= (A(\mathbb{G})\otimes f)\circ\beta_{\mathcal{V}(\mathbb{G})}(Y)\end{aligned}$$

e para cada $h\in G$:

$$\begin{aligned}(\beta_u\otimes A^v_{\tau,b}(\mathbb{G}))\circ f(W_h) &= (\beta_u\otimes A^v_{\tau,b}(\mathbb{G}))(T_{v(h)}\otimes T_h)\\ &= u(v(h))\otimes T_{v(h)}\otimes T_h\\ &= (A(\mathbb{G})\otimes f)(u(v(h))\otimes W_h)\\ &= (A(\mathbb{G})\otimes f)\circ\beta_{\mathcal{V}(\mathbb{G})}(W_h)\end{aligned}$$

Portanto f é morfismo de $A(\mathbb{G})$-bicomódulos.

Pela Proposição 1.19, temos um morfismo de $A(\mathbb{G})$-bicomódulo álgebras:

$$\begin{aligned}f'\colon \mathcal{L}(\mathbb{G}) &\longrightarrow A^u_{\sigma,a}(\mathbb{G})\underset{A(\mathbb{G})}{\square} A^v_{\tau,b}(\mathbb{G})\\ Y &\longmapsto 1\otimes X + X\otimes T_g\\ W_h &\longmapsto T_{v(h)}\otimes T_h\end{aligned}$$

Durante a demonstração da Proposição 2.15, mostramos que $\mathcal{I}_{\omega,c}(\mathbb{G})$ é $A(\mathbb{G})$-subcomódulo à direita de $\mathcal{L}(\mathbb{G})$.

Durante a demonstração da Proposição 3.3, mostramos que, se $u\circ v\in \mathrm{Aut}_g(G)$ satisfaz a condição:

$$\chi\circ(u\circ v)(h) = \omega(g,h)^{-1}\omega(h,g)\chi(h),\ \forall h\in G$$

então $\mathcal{I}_{\omega,c}(\mathbb{G})$ é $A(\mathbb{G})$-subcomódulo à esquerda de $\mathcal{L}(\mathbb{G})$.

Pelo Corolário 1.21, temos um morfismo de $A(\mathbb{G})$-bicomódulo álgebras:

$$\begin{aligned} F\colon A^{u\circ v}_{\omega,c}(\mathbb{G}) &\longrightarrow A^{u}_{\sigma,a}(\mathbb{G}) \underset{A(\mathbb{G})}{\square} A^{v}_{\tau,b}(\mathbb{G}) \\ X &\longmapsto 1\otimes X + X\otimes T_g \\ T_h &\longmapsto T_{v(h)}\otimes T_h \end{aligned}$$

Como $A^{u\circ v}_{\omega,c}(\mathbb{G})$ e $A^{u}_{\sigma,a}(\mathbb{G}) \underset{A(\mathbb{G})}{\square} A^{v}_{\tau,b}(\mathbb{G})$ são objetos $A(\mathbb{G})$-biGalois, segue que F é isomorfismo. $\square$

3.2 O grupo $\Gamma(\mathbb{G})$

Observação 3.6. *O conjunto $Aut_g(G)$ tem uma ação à esquerda sobre $H^2_{1,g}(G,\mathbb{K}^*)$ dada por:*

$$\begin{aligned} Aut_g(G)\times H^2_{1,g}(G,\mathbb{K}^*) &\longrightarrow H^2_{1,g}(G,\mathbb{K}^*) \\ u\times\overline{\sigma} &\longmapsto \overline{\sigma\circ(u\times u)} \end{aligned}$$

Logo, temos o produto semi-direto $Aut_g(G)\ltimes H^2_{1,g}(G,\mathbb{K}^*)$, que é grupo com multiplicação dada por:

$$\begin{aligned} (u,\overline{\sigma})(v,\overline{\tau}) &= (u,\overline{(v\cdot\sigma)\tau}) \\ &= (u\circ v,\overline{(\sigma\circ(v\times v))\tau}) \end{aligned}$$

Definição 3.7. *Seja $\mathbb{G}=(G,g,\chi,\mu)$ um conjunto de dados de grupo. Definimos o conjunto $\Gamma(\mathbb{G})$ por:*

$$\Gamma(\mathbb{G}) = \big\{(u,\overline{\sigma})\in Aut_g(G)\ltimes H^2_{1,g}(G,\mathbb{K}^*);\chi\circ u(h)=\sigma(g,h)^{-1}\sigma(h,g)\chi(h),\ \forall h\in G\big\}$$

Proposição 3.8. *O conjunto $\Gamma(\mathbb{G})$ é subgrupo de $Aut_g(G)\ltimes H^2_{1,g}(G,\mathbb{K}^*)$.*

Demonstração. Sejam $(u,\overline{\sigma}),(v,\overline{\tau})\in\Gamma(\mathbb{G})$. Vejamos que $(u\circ v,\overline{(v\cdot\sigma)\tau})\in\Gamma(\mathbb{G})$. De fato, temos que:

$$\begin{aligned} \chi\circ u\circ v(h) &= \sigma(g,v(h))^{-1}\sigma(v(h),g)\chi(v(h)) \\ &= \sigma(v(g),v(h))^{-1}\sigma(v(h),v(g))\tau(g,h)^{-1}\tau(h,g)\chi(h) \\ &= ((v\cdot\sigma)\tau)(g,h)^{-1}((v\cdot\sigma)\tau)(h,g)\chi(h) \end{aligned}$$

O elemento neutro de $\mathrm{Aut}_g(G)\ltimes H^2_{1,g}(G,\mathbb{K}^*)$ é $(1_G,\overline{1})$, onde 1_G é o morfismo identidade de G e $1\colon G\times G\to\mathbb{K}^*$ é o morfismo constante $1(g,h)=1$. Temos que:

$$\begin{aligned} \chi\circ 1_G(h) &= \chi(h) \\ &= 1(g,h)^{-1}1(h,g)\chi(h) \end{aligned}$$

Portanto $(1_G,\overline{1})\in\Gamma(\mathbb{G})$.

Seja $(u,\overline{\sigma})\in\Gamma(\mathbb{G})$ um elemento qualquer. A inversa de $(u,\overline{\sigma})$ em $\mathrm{Aut}_g(G)\ltimes H^2_{1,g}(G,\mathbb{K}^*)$ é dada por $(u^{-1},\overline{(\sigma\circ(u^{-1}\times u^{-1}))^{-1}})$, pois pela direita, temos:

$$\begin{aligned} (u,\overline{\sigma})(u^{-1},\overline{(\sigma\circ(u^{-1}\times u^{-1}))^{-1}}) &= (u\circ u^{-1},\overline{(u^{-1}\cdot\sigma)(\sigma\circ(u^{-1}\times u^{-1}))^{-1}}) \\ &= (u\circ u^{-1},\overline{(\sigma\circ(u^{-1}\times u^{-1}))(\sigma\circ(u^{-1}\times u^{-1}))^{-1}}) \\ &= (1_G,\overline{1}) \end{aligned}$$

e se a inversa existe, então a inversa pela direita é igual à inversa pela esquerda.

Note que:

$$\begin{aligned} \chi(h) &= \chi \circ u \circ u^{-1}(h) \\ &= \sigma(g, u^{-1}(h))^{-1}\sigma(u^{-1}(h), g)\chi \circ u^{-1}(h) \end{aligned}$$

Logo, temos que:

$$\begin{aligned} \chi \circ u^{-1}(h) &= \sigma(u^{-1}(h), g)^{-1}\sigma(g, u^{-1}(h))\chi(h) \\ &= \sigma(u^{-1}(h), u^{-1}(g))^{-1}\sigma(u^{-1}(g), u^{-1}(h))\chi(h) \\ &= \big((\sigma \circ (u^{-1} \times u^{-1}))^{-1}\big)(g, h)^{-1}\big((\sigma \circ (u^{-1} \times u^{-1}))^{-1}\big)(h, g)\chi(h) \end{aligned}$$

e $(u^{-1}, \overline{(\sigma \circ (u^{-1} \times u^{-1}))^{-1}}) \in \Gamma(\mathbb{G})$.

Portanto $\Gamma(\mathbb{G})$ é subgrupo de $\mathrm{Aut}_g(G) \ltimes H^2_{1,g}(G, \mathbb{K}^*)$. □

3.3 Descrição dos objetos $A(\mathbb{G})$-biGalois com $\mathbb{G}$ do tipo I e II

Proposição 3.9. *Sejam $\mathbb{G} = (G, g, \chi)$ um conjunto de dados de grupo do tipo I ou II e $\sigma \in Z^2(G, \mathbb{K}^*)$. Então existe $u \in Aut_g(G)$ tal que $(u, \overline{\sigma}) \in \Gamma(\mathbb{G})$.*

Demonstração. Como $d = o(\chi(g)) = o(g)$, a função χ induz um isomorfismo de grupos entre $\langle g \rangle$ e o grupo das d-ésimas raízes da unidade em $\mathbb{K}$, que denotaremos por Ω_d. Seja $s\colon \Omega_d \to \langle g \rangle$ a inversa da restrição de χ à $\langle g \rangle$.

Como para todo i, temos que:

$$\big(\sigma(g, h)^{-1}\sigma(h, g)\big)^i = \sigma(g^i, h)^{-1}\sigma(h, g^i)$$

considere a função:

$$\begin{aligned} f\colon G &\longrightarrow \Omega_d \\ h &\longmapsto \sigma(g, h)^{-1}\sigma(h, g) \end{aligned}$$

Como $\sigma \in Z^2(G, \mathbb{K}^*)$, temos que:

$$\begin{aligned} f(h_1h_2) &= \sigma(g, h_1h_2)^{-1}\sigma(h_1h_2, g) \\ &= \sigma(h_1, h_2)\sigma(gh_1, h_2)^{-1}\sigma(g, h_1)^{-1}\sigma(h_1, h_2)^{-1}\sigma(h_1, h_2g)\sigma(h_2, g) \\ &= \sigma(g, h_1)^{-1}\sigma(h_1g, h_2)^{-1}\sigma(h_1, gh_2)\sigma(h_2, g) \\ &= \sigma(g, h_1)^{-1}\sigma(h_1, g)\sigma(h_1, gh_2)^{-1}\sigma(g, h_2)^{-1}\sigma(h_1, gh_2)\sigma(h_2, g) \\ &= \sigma(g, h_1)^{-1}\sigma(h_1, g)\sigma(g, h_2)^{-1}\sigma(h_2, g) \\ &= f(h_1)f(h_2) \end{aligned}$$

Portanto f é morfismo de grupos. Note que $f(g) = 1$.

Defina a função $u\colon G \to G$ por:

$$u(h) = s(f(h))h, \ \forall h \in G$$

Como s e f são morfismos de grupos e g é central, temos que para $h_1, h_2 \in G$:

$$\begin{aligned} u(h_1h_2) &= s(f(h_1h_2))h_1h_2 \\ &= s(f(h_1))s(f(h_2))h_1h_2 \\ &= s(f(h_1))h_1s(f(h_2))h_2 \\ &= u(h_1)u(h_2) \end{aligned}$$

Portanto u é morfismo de grupos. Temos que $u(g) = s(f(g))g = s(1)g = g$. Logo $u\big((s(f(h)))^{-1}\big) = s(f(h))^{-1}$, $\forall h \in G$, o que implica que:

$$\begin{aligned} u\big((s(f(h)))^{-1}h\big) &= u((s(f(h)))^{-1})u(h) \\ &= (s(f(h)))^{-1}s(f(h))h \\ &= h \end{aligned}$$

e u é sobrejetor. Como G é finito, temos que $u \in \mathrm{Aut}_g(G)$.

Além disso, temos que:

$$\chi \circ u(h) = \sigma(g,h)^{-1}\sigma(h,g)\chi(h),\ \forall h \in G$$

□

Observação 3.10. *O conjunto $H^2_{1,g}(G,\mathbb{K}^*)$ tem uma ação sobre $\mathbb{K}$ dada por:*

$$\begin{aligned} H^2_{1,g}(G,\mathbb{K}^*) \otimes \mathbb{K} &\longrightarrow \mathbb{K} \\ \overline{\sigma} \otimes a &\longmapsto \sigma(g,g)\cdots\sigma(g,g^{d-1})a \end{aligned}$$

Podemos estender esta ação naturalmente para $\Gamma(\mathbb{G})$.

Proposição 3.11. *Seja $\mathbb{G} = (G,g,\chi)$ um conjunto de dados de grupo do tipo I. Então temos um isomorfismo de grupos:*

$$BiGal(A(\mathbb{G})) \cong \Gamma(\mathbb{G}) \ltimes \mathbb{K}$$

Demonstração. Considere a seguinte função:

$$\begin{aligned} \Psi\colon \Gamma(\mathbb{G}) \ltimes \mathbb{K} &\longrightarrow \mathrm{BiGal}(A(\mathbb{G})) \\ (u,\overline{\sigma},a) &\longmapsto \big[A^u_{\sigma,a}(\mathbb{G})\big] \end{aligned}$$

Pela Proposição 3.3, temos que $A^u_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois para todo $(u,\overline{\sigma}) \in \Gamma(\mathbb{G})$ e $a \in \mathbb{K}$. Logo, a função Ψ está bem definida.

Pela Proposição 3.4, a função Ψ é injetora.

Pela Proposição 3.5, a função Ψ é morfismo de grupos.

Precisamos verificar que Ψ é sobrejetora. Seja Z um objeto $A(\mathbb{G})$-biGalois. Em particular, Z é um objeto $A(\mathbb{G})$-Galois à direita e, pela Proposição 2.25, existem $\sigma \in Z^2(G,\mathbb{K}^*)$ e $a \in \mathbb{K}$ tais que $Z = A_{\sigma,a}(\mathbb{G})$ como $A(\mathbb{G})$-comódulo álgebras à direita. Seja ρ a coação à direita de $A(\mathbb{G})$ sobre Z.

Pela Proposição 3.9, existe $u \in \mathrm{Aut}_g(G)$ tal que $(u,\overline{\sigma}) \in \Gamma(\mathbb{G})$. Pela Proposição 3.3, temos que $A^u_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois.

Pelo Teorema 1.83, existe $f \in \mathrm{Aut}_{Hopf}(A(\mathbb{G}))$ tal que, se β é a coação à esquerda de Z e β_u é a coação à esquerda de $A^u_{\sigma,a}(\mathbb{G})$, então $\beta = (f \otimes Z) \circ \beta_u$. Diremos que $Z = {}^f A^u_{\sigma,a}(\mathbb{G})$.

Pela Proposição 2.10, existem $v \in \mathrm{Aut}_{g,\chi}(G)$ e $r \in \mathbb{K}^*$ tais que $f(x) = rx$ e $f(h) = v(h)$, $\forall h \in G$. Considere uma função $\theta\colon G \to \mathbb{K}^*$ com $\theta(1) = 1$ e $\theta(g) = r$.

Como g é central, para cada $i \geq 0$, temos que:

$$\begin{aligned} \partial(\theta)(g^i,h) &= \theta(h)\theta(g^ih)^{-1}\theta(g^i) \\ &= \theta(g^i)\theta(hg^i)^{-1}\theta(h) \\ &= \partial(\theta)(h,g^i) \end{aligned}$$

Logo, como $A_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois, temos que:

$$\begin{aligned}
a(\partial(\theta)\sigma)(g^d,h) &= a\sigma(g^d,h)\partial(\theta)(g^d,h)\\
&= a\chi(h)^d\sigma(h,g^d)\partial(\theta)(g^d,h)\\
&= a\chi(h)^d\sigma(h,g^d)\partial(\theta)(h,g^d)\\
&= a\chi(h)^d(\partial(\theta)\sigma)(h,g^d)
\end{aligned}$$

e $A_{\partial(\theta)\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois.

Como $u \in \mathrm{Aut}_g(G)$ e $v \in \mathrm{Aut}_{g,\chi}(G) \subset \mathrm{Aut}_g(G)$, temos que $v \circ u \in \mathrm{Aut}_g(G)$. Além disso, temos que:

$$\begin{aligned}
\chi \circ v \circ u(h) &= \chi \circ u(h)\\
&= \sigma(g,h)^{-1}\sigma(h,g)\chi(h)\\
&= \sigma(g,h)^{-1}\partial(\theta)(g,h)^{-1}\partial(\theta)(g,h)\sigma(h,g)\chi(h)\\
&= \sigma(g,h)^{-1}\partial(\theta)(g,h)^{-1}\partial(\theta)(h,g)\sigma(h,g)\chi(h)
\end{aligned}$$

Logo, $(v \circ u, \overline{\partial(\theta)\sigma}) \in \Gamma(\mathbb{G})$ e $A^{v\circ u}_{\partial(\theta)\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois.

Considere a função:

$$\begin{aligned}
\phi\colon \mathcal{V}(\mathbb{G}) &\longrightarrow {}^f A^u_{\sigma,a}(\mathbb{G})\\
Y &\longmapsto X\\
W_h &\longmapsto \theta(h)T_h
\end{aligned}$$

onde $\mathcal{V}(\mathbb{G})$ é $A(\mathbb{G})$-bicomódulo com estrutura à direita dada por:

$$\begin{aligned}
\rho_{\mathcal{V}(\mathbb{G})}\colon \mathcal{V}(\mathbb{G}) &\longrightarrow \mathcal{V}(\mathbb{G}) \otimes A(\mathbb{G})\\
Y &\longmapsto 1 \otimes x + Y \otimes g\\
W_h &\longmapsto W_h \otimes h
\end{aligned}$$

e estrutura à esquerda dada por:

$$\begin{aligned}
\beta_{\mathcal{V}(\mathbb{G})}\colon \mathcal{V}(\mathbb{G}) &\longrightarrow A(\mathbb{G}) \otimes \mathcal{V}(\mathbb{G})\\
Y &\longmapsto 1 \otimes Y + x \otimes T_g\\
W_h &\longmapsto v \circ u(h) \otimes W_h
\end{aligned}$$

Vejamos que ϕ é morfismo de $A(\mathbb{G})$-comódulos à direita:

$$\begin{aligned}
\rho \circ \phi(Y) &= \rho(X)\\
&= 1 \otimes x + X \otimes g\\
&= (\phi \otimes A(\mathbb{G}))(1 \otimes x + Y \otimes g)\\
&= (\phi \otimes A(\mathbb{G})) \circ \rho_{\mathcal{V}(\mathbb{G})}(Y)
\end{aligned}$$

e para cada $h \in G$:

$$\begin{aligned}
\rho \circ \phi(W_h) &= \rho(\theta(h)T_h)\\
&= \theta(h)T_h \otimes h\\
&= (\phi \otimes A(\mathbb{G}))(W_h \otimes h)\\
&= (\phi \otimes A(\mathbb{G})) \circ \rho_{\mathcal{V}(\mathbb{G})}(W_h)
\end{aligned}$$

Vejamos que ϕ é morfismo de $A(\mathbb{G})$-comódulos à esquerda:

$$\begin{aligned}
\beta \circ \phi(Y) &= (f \otimes Z) \circ \beta_u(X) \\
&= (f \otimes Z)(1 \otimes X + x \otimes T_g) \\
&= f(1) \otimes X + f(x) \otimes T_g \\
&= 1 \otimes X + rx \otimes T_g \\
&= 1 \otimes X + \theta(g)x \otimes T_g \\
&= (A(\mathbb{G}) \otimes \phi)(1 \otimes Y + x \otimes W_g) \\
&= (A(\mathbb{G}) \otimes \phi) \circ \beta_{\mathcal{V}(\mathbb{G})}(Y)
\end{aligned}$$

e para cada $h \in G$:

$$\begin{aligned}
\beta \circ \phi(W_h) &= (f \otimes Z) \circ \beta_u(\theta(h)T_h) \\
&= (f \otimes Z)(\theta(h)u(h) \otimes T_h) \\
&= \theta(h)f(u(h)) \otimes T_h \\
&= \theta(h)v \circ u(h) \otimes T_h \\
&= (A(\mathbb{G}) \otimes \phi)(v \circ u(h) \otimes W_h) \\
&= (A(\mathbb{G}) \otimes \phi) \circ \beta_{\mathcal{V}(\mathbb{G})}(W_h)
\end{aligned}$$

Portanto ϕ é morfismo de $A(\mathbb{G})$-bicomódulos.

Pela Proposição 1.19, temos um morfismo de $A(\mathbb{G})$-bicomódulo álgebras:

$$\begin{aligned}
\phi' \colon \mathcal{L}(\mathbb{G}) &\longrightarrow {}^f A^u_{\sigma,a}(\mathbb{G}) \\
Y &\longmapsto X \\
W_h &\longmapsto \theta(h)T_h
\end{aligned}$$

Durante a demonstração da Proposição 2.15, mostramos que $\mathcal{I}_{\partial(\theta)\sigma,a}(\mathbb{G})$ é $A(\mathbb{G})$-subcomódulo à direita de $\mathcal{L}(\mathbb{G})$.

Durante a demonstração da Proposição 3.3, mostramos que, se $v \circ u \in \mathrm{Aut}_g(G)$ satisfaz a condição:

$$\chi \circ (v \circ u)(h) = (\partial(\theta)\sigma)(g,h)^{-1}(\partial(\theta)\sigma)(h,g)\chi(h), \ \forall h \in G$$

então $\mathcal{I}_{\partial(\theta)\sigma,a}(\mathbb{G})$ é $A(\mathbb{G})$-subcomódulo à esquerda de $\mathcal{L}(\mathbb{G})$.

Pelo Corolário 1.21, temos um morfismo de $A(\mathbb{G})$-bicomódulo álgebras:

$$\begin{aligned}
F \colon A^{v \circ u}_{\partial(\theta)\sigma,a}(\mathbb{G}) &\longrightarrow {}^f A^u_{\sigma,a}(\mathbb{G}) \\
X &\longmapsto X \\
T_h &\longmapsto \theta(h)T_h
\end{aligned}$$

Como $A^{v \circ u}_{\partial(\theta)\sigma,a}(\mathbb{G})$ e ${}^f A^u_{\sigma,a}(\mathbb{G})$ são objetos $A(\mathbb{G})$-biGalois, segue que F é isomorfismo e $\left[A^{v \circ u}_{\partial(\theta)\sigma,a}(\mathbb{G})\right] = [Z]$. Portanto Ψ é sobrejetora. □

Proposição 3.12. *Seja $\mathbb{G} = (G, g, \chi)$ um conjunto de dados de grupo do tipo II. Então temos um isomorfismo de grupos:*

$$BiGal(A(\mathbb{G})) \cong \Gamma(\mathbb{G})$$

Demonstração. Considere a função:

$$\begin{aligned}
\Psi \colon \Gamma(\mathbb{G}) &\longrightarrow \mathrm{BiGal}(A(\mathbb{G})) \\
(u, \overline{\sigma}) &\longmapsto \left[A^u_{\sigma,0}(\mathbb{G})\right]
\end{aligned}$$

Pela Proposição 3.3, temos que $A^u_{\sigma,0}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois para todo $(u,\overline{\sigma}) \in \Gamma(\mathbb{G})$. Logo, a função Ψ está bem definida.

Pela Proposição 3.4, a função Ψ é injetora.

Pela Proposição 3.5, a função Ψ é morfismo de grupos.

Precisamos verificar que Ψ é sobrejetora. Seja Z um objeto $A(\mathbb{G})$-biGalois. Em particular, Z é um objeto $A(\mathbb{G})$-Galois à direita e, pela Proposição 2.26, existe $\sigma \in Z^2(G,\mathbb{K}^*)$ tal que $Z = A_{\sigma,0}(\mathbb{G})$ como $A(\mathbb{G})$-comódulo álgebras à direita.

Pela Proposição 3.9, existe $u \in \mathrm{Aut}_g(G)$ tal que $(u,\overline{\sigma}) \in \Gamma(\mathbb{G})$. Pela Proposição 3.3, temos que $A^u_{\sigma,0}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois.

Pelo Teorema 1.83, existe $f \in \mathrm{Aut}_{Hopf}(A(\mathbb{G}))$ tal que, se β é a coação à esquerda de Z e β_u é a coação à esquerda de $A^u_{\sigma,0}(\mathbb{G})$, então $\beta = (f \otimes Z) \circ \beta_u$. Diremos que $Z = {}^f A^u_{\sigma,0}(\mathbb{G})$.

Pela Proposição 2.10, existem $v \in \mathrm{Aut}_{g,\chi}(G)$ e $r \in \mathbb{K}^*$ tais que $f(x) = rx$ e $f(h) = v(h)$, $\forall h \in G$. Considere uma função $\theta\colon G \to \mathbb{K}^*$ com $\theta(1) = 1$ e $\theta(g) = r$.

Claramente $A_{\partial(\theta)\sigma,0}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois.

Como g é central, temos que:

$$\begin{aligned}\partial(\theta)(g,h) &= \theta(h)\theta(gh)^{-1}\theta(g)\\ &= \theta(g)\theta(hg)^{-1}\theta(h)\\ &= \partial(\theta)(h,g)\end{aligned}$$

Como $u \in \mathrm{Aut}_g(G)$ e $v \in \mathrm{Aut}_{g,\chi}(G) \subset \mathrm{Aut}_g(G)$, temos que $v \circ u \in \mathrm{Aut}_g(G)$. Além disso, temos que:

$$\begin{aligned}\chi \circ v \circ u(h) &= \chi \circ u(h)\\ &= \sigma(g,h)^{-1}\sigma(h,g)\chi(h)\\ &= \sigma(g,h)^{-1}\partial(\theta)(g,h)^{-1}\partial(\theta)(g,h)\sigma(h,g)\chi(h)\\ &= \sigma(g,h)^{-1}\partial(\theta)(g,h)^{-1}\partial(\theta)(h,g)\sigma(h,g)\chi(h)\end{aligned}$$

Logo, $(v \circ u, \overline{\partial(\theta)\sigma}) \in \Gamma(\mathbb{G})$ e $A^{v\circ u}_{\partial(\theta)\sigma,0}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois.

Considere a função:

$$\begin{aligned}\phi\colon \mathcal{V}(\mathbb{G}) &\longrightarrow {}^f A^u_{\sigma,0}(\mathbb{G})\\ Y &\longmapsto X\\ W_h &\longmapsto \theta(h)T_h\end{aligned}$$

onde $\mathcal{V}(\mathbb{G})$ é $A(\mathbb{G})$-bicomódulo com estrutura à direita dada por:

$$\begin{aligned}\rho_{\mathcal{V}(\mathbb{G})}\colon \mathcal{V}(\mathbb{G}) &\longrightarrow \mathcal{V}(\mathbb{G}) \otimes A(\mathbb{G})\\ Y &\longmapsto 1 \otimes x + Y \otimes g\\ W_h &\longmapsto W_h \otimes h\end{aligned}$$

e estrutura à esquerda dada por:

$$\begin{aligned}\beta_{\mathcal{V}(\mathbb{G})}\colon \mathcal{V}(\mathbb{G}) &\longrightarrow A(\mathbb{G}) \otimes \mathcal{V}(\mathbb{G})\\ Y &\longmapsto 1 \otimes Y + x \otimes T_g\\ W_h &\longmapsto v \circ u(h) \otimes W_h\end{aligned}$$

Vejamos que ϕ é morfismo de $A(\mathbb{G})$-comódulos à direita:

$$\begin{aligned}\rho \circ \phi(Y) &= \rho(X)\\ &= 1 \otimes x + X \otimes g\\ &= (\phi \otimes A(\mathbb{G}))(1 \otimes x + Y \otimes g)\\ &= (\phi \otimes A(\mathbb{G})) \circ \rho_{\mathcal{V}(\mathbb{G})}(Y)\end{aligned}$$

e para cada $h \in G$:

$$\begin{aligned}\rho \circ \phi(W_h) &= \rho(\theta(h)T_h)\\ &= \theta(h)T_h \otimes h\\ &= (\phi \otimes A(\mathbb{G}))(W_h \otimes h)\\ &= (\phi \otimes A(\mathbb{G})) \circ \rho_{\mathcal{V}(\mathbb{G})}(W_h)\end{aligned}$$

Vejamos que ϕ é morfismo de $A(\mathbb{G})$-comódulos à esquerda:

$$\begin{aligned}\beta \circ \phi(Y) &= (f \otimes Z) \circ \beta_u(X)\\ &= (f \otimes Z)(1 \otimes X + x \otimes T_g)\\ &= f(1) \otimes X + f(x) \otimes T_g\\ &= 1 \otimes X + rx \otimes T_g\\ &= 1 \otimes X + \theta(g)x \otimes T_g\\ &= (A(\mathbb{G}) \otimes \phi)(1 \otimes Y + x \otimes W_g)\\ &= (A(\mathbb{G}) \otimes \phi) \circ \beta_{\mathcal{V}(\mathbb{G})}(Y)\end{aligned}$$

e para cada $h \in G$:

$$\begin{aligned}\beta \circ \phi(W_h) &= (f \otimes Z) \circ \beta_u(\theta(h)T_h)\\ &= (f \otimes Z)(\theta(h)u(h) \otimes T_h)\\ &= \theta(h)f(u(h)) \otimes T_h\\ &= \theta(h)v \circ u(h) \otimes T_h\\ &= (A(\mathbb{G}) \otimes \phi)(v \circ u(h) \otimes W_h)\\ &= (A(\mathbb{G}) \otimes \phi) \circ \beta_{\mathcal{V}(\mathbb{G})}(W_h)\end{aligned}$$

Portanto ϕ é morfismo de $A(\mathbb{G})$-bicomódulos.

Pela Proposição 1.19, temos um morfismo de $A(\mathbb{G})$-bicomódulo álgebras:

$$\begin{aligned}\phi' \colon \mathcal{L}(\mathbb{G}) &\longrightarrow {}^f A^u_{\sigma,0}(\mathbb{G})\\ Y &\longmapsto X\\ W_h &\longmapsto \theta(h)T_h\end{aligned}$$

Durante a demonstração da Proposição 2.15, mostramos que $\mathcal{I}_{\partial(\theta)\sigma,0}(\mathbb{G})$ é $A(\mathbb{G})$-subcomódulo à direita de $\mathcal{L}(\mathbb{G})$.

Durante a demonstração da Proposição 3.3, mostramos que, se $v \circ u \in \mathrm{Aut}_g(G)$ satisfaz a condição:

$$\chi \circ (v \circ u)(h) = (\partial(\theta)\sigma)(g,h)^{-1}(\partial(\theta)\sigma)(h,g)\chi(h),\ \forall h \in G$$

então $\mathcal{I}_{\partial(\theta)\sigma,0}(\mathbb{G})$ é $A(\mathbb{G})$-subcomódulo à esquerda de $\mathcal{L}(\mathbb{G})$.

Pelo Corolário 1.21, temos um morfismo de $A(\mathbb{G})$-bicomódulo álgebras:

$$\begin{aligned}F \colon A^{v\circ u}_{\partial(\theta)\sigma,0}(\mathbb{G}) &\longrightarrow {}^f A^u_{\sigma,0}(\mathbb{G})\\ X &\longmapsto X\\ T_h &\longmapsto \theta(h)T_h\end{aligned}$$

Como $A^{v\circ u}_{\partial(\theta)\sigma,0}(\mathbb{G})$ e ${}^f A^u_{\sigma,0}(\mathbb{G})$ são objetos $A(\mathbb{G})$-biGalois, segue que F é isomorfismo e $\left[A^{v\circ u}_{\partial(\theta)\sigma,0}(\mathbb{G})\right] = [Z]$. Portanto Ψ é sobrejetora. $\square$

3.4 Os objetos $A(\mathbb{G}')$-$A(\mathbb{G})$-biGalois

A existência de $u \in \mathrm{Aut}_g(G)$ tal que $A^u_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois quando $\mathbb{G}$ é do tipo I ou II é feito na Proposição 3.9, mas não há um resultado equivalente para os demais casos. Precisamos utilizar o segundo caso apresentado na Observação 3.2. Nesta seção apresentaremos as condições sobre $\mathbb{G}'$ para que $A_{\sigma,a}(\mathbb{G})$ seja objeto $A(\mathbb{G}')$-$A(\mathbb{G})$-biGalois. Esta estrutura é essencial para resolvermos o Teorema 3.1 para conjuntos de dados de grupo do tipo III e IV.

Na proposição a seguir, tomamos $g^d \neq 1$ pois quando $g^d = 1$ temos que $\mathbb{G}$ é do tipo I ou II e os casos I e II já foram resolvidos. Sem esta condição, não teríamos a equação $\mu = -a\sigma(g,g)^{-1}\cdots\sigma(g,g^{d-1})^{-1}$.

Proposição 3.13. *Sejam $\mathbb{G} = (G,g,\chi)$ e $\mathbb{G}' = (G,g,\chi',\mu)$ dois conjuntos de dados de grupo com $g^d \neq 1$, $\sigma \in Z^2(G,\mathbb{K}^*)$ e $a \in \mathbb{K}$ tais que $A_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois. Então $A_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G}')$-$A(\mathbb{G})$-biGalois com coação à esquerda dada por:*

$$\begin{aligned}\beta\colon A_{\sigma,a}(\mathbb{G}) &\longrightarrow A(\mathbb{G}')\otimes A_{\sigma,a}(\mathbb{G})\\ X &\longmapsto 1\otimes X + x\otimes T_g\\ T_h &\longmapsto h\otimes T_h,\ \forall h\in G\end{aligned}$$

se, e somente se:

$$\begin{aligned}\chi'(h) &= \sigma(g,h)^{-1}\sigma(h,g)\chi(h),\ \forall h\in G\\ \mu &= -a\sigma(g,g)^{-1}\cdots\sigma(g,g^{d-1})^{-1}\end{aligned}$$

Demonstração. ($\Rightarrow$) Como β está bem definido, temos que $\beta(XT_h) = \beta(\chi(h)T_hX)$, $\forall h \in G$. Mas:

$$\begin{aligned}\beta(XT_h) &= (1\otimes X + x\otimes T_g)(h\otimes T_h)\\ &= h\otimes XT_h + xh\otimes T_gT_h\\ &= \chi(h)h\otimes T_hX + \chi'(h)\sigma(g,h)hx\otimes T_{gh}\end{aligned}$$

e:

$$\begin{aligned}\beta(\chi(h)T_hX) &= \chi(h)(h\otimes T_h)(1\otimes X + x\otimes T_g)\\ &= \chi(h)h\otimes T_hX + \chi(h)hx\otimes T_hT_g\\ &= \chi(h)h\otimes T_hX + \chi(h)\sigma(h,g)hx\otimes T_{gh}\end{aligned}$$

Como o conjunto:

$$\{h_1x^i\otimes T_{h_2}X^j;\ h_1,h_2\in G, 0\le i,j\le d-1\}$$

é base de $A(\mathbb{G}')\otimes A_{\sigma,a}(\mathbb{G})$, temos que $\chi'(h)\sigma(g,h) = \chi(h)\sigma(h,g)$, $\forall h\in G$.

Também temos que $\beta(X^d) = \beta(aT_{g^d})$. Mas, por um lado, temos:

$$\begin{aligned}\beta(X^d) &= (1\otimes X + x\otimes T_g)^d\\ &\overset{\text{Corolário A.8}}{=} 1\otimes X^d + x^d\otimes (T_g)^d\\ &= a1\otimes T_{g^d} + \mu\sigma(g,g)\cdots\sigma(g,g^{d-1})(1-g^d)\otimes T_{g^d}\\ &= (a1 + \mu\sigma(g,g)\cdots\sigma(g,g^{d-1})(1-g^d))\otimes T_{g^d}\end{aligned}$$

e por outro lado:

$$\beta(aT_{g^d}) = ag^d\otimes T_{g^d}$$

Logo $ag^d = a1 + \mu\sigma(g,g)\cdots\sigma(g,g^{d-1})(1-g^d)$. Simplificando, temos:

$$-a(1-g^d) = \mu\sigma(g,g)\cdots\sigma(g,g^{d-1})(1-g^d)$$

Como $g^d \neq 1$, temos que $\mu = -a\sigma(g,g)^{-1}\cdots\sigma(g,g^{d-1})^{-1}$.
($\Leftarrow$) Vejamos que $\mathcal{V}(\mathbb{G})$ é $A(\mathbb{G})$-comódulo à esquerda com:

$$\begin{aligned} f\colon \mathcal{V}(\mathbb{G}) &\longrightarrow A(\mathbb{G}) \otimes \mathcal{V}(\mathbb{G}) \\ Y &\longmapsto 1 \otimes Y + x \otimes W_g \\ W_h &\longmapsto h \otimes W_h,\ \forall h \in G \end{aligned}$$

De fato, temos:

$$\begin{aligned} (A(\mathbb{G}) \otimes f) \circ f(Y) &= (A(\mathbb{G}) \otimes f)(1 \otimes Y + x \otimes W_g) \\ &= 1 \otimes (1 \otimes Y + x \otimes W_g) + x \otimes g \otimes W_g \\ &= 1 \otimes 1 \otimes Y + 1 \otimes x \otimes W_g + x \otimes g \otimes W_g \\ &= (\Delta_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G}))(1 \otimes Y) + (\Delta_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G}))(x \otimes W_g) \\ &= (\Delta_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G})) \circ f(Y) \end{aligned}$$

e para cada $h \in G$ temos:

$$\begin{aligned} (A(\mathbb{G}) \otimes f) \circ f(W_h) &= (A(\mathbb{G}) \otimes f)(h \otimes W_h) \\ &= h \otimes h \otimes W_h \\ &= (\Delta \otimes \mathcal{V}(\mathbb{G}))(h \otimes W_h) \\ &= (\Delta_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G})) \circ f(W_h) \end{aligned}$$

Além disso, como $\varepsilon_{A(\mathbb{G})}(h) = 1, \forall h \in G$ e $\varepsilon_{A(\mathbb{G})}(x) = 0$, temos:

$$\begin{aligned} (\varepsilon_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G})) \circ f(Y) &= (\varepsilon_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G}))(1 \otimes Y + x \otimes W_g) \\ &= \varepsilon_{A(\mathbb{G})}(1) \otimes Y + \varepsilon_{A(\mathbb{G})}(x) \otimes W_g \\ &= 1 \otimes Y \end{aligned}$$

e para cada $h \in G$ temos:

$$\begin{aligned} (\varepsilon_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G})) \circ f(W_h) &= (\varepsilon_{A(\mathbb{G})} \otimes \mathcal{V}(\mathbb{G}))(h \otimes W_h) \\ &= \varepsilon_{A(\mathbb{G})}(h) \otimes W_h \\ &= 1 \otimes W_h \end{aligned}$$

Portanto $\mathcal{V}(\mathbb{G})$ é $A(\mathbb{G})$-comódulo com a estrutura acima.
Pela Teorema 1.10, $\mathcal{L}(\mathbb{G})$ é $A(\mathbb{G})$-comódulo álgebra com coação dada por:

$$\begin{aligned} f'\colon \mathcal{L}(\mathbb{G}) &\longrightarrow A(\mathbb{G}) \otimes \mathcal{L}(\mathbb{G}) \\ Y &\longmapsto 1 \otimes Y + x \otimes W_g \\ W_h &\longmapsto h \otimes W_h,\ \forall h \in G \end{aligned}$$

Vejamos que $f'(\mathcal{I}_{\sigma,a}(\mathbb{G})) \subset A(\mathbb{G}) \otimes \mathcal{I}_{\sigma,a}(\mathbb{G})$. De fato, nos geradores de $\mathcal{I}_{\sigma,a}(\mathbb{G})$, temos:

$$\begin{aligned} f'(W_{h_1}W_{h_2} - \sigma(h_1,h_2)W_{h_1h_2}) &= h_1h_2 \otimes W_{h_1}W_{h_2} - \sigma(h_1,h_2)h_1h_2 \otimes W_{h_1h_2} \\ &= h_1h_2 \otimes (W_{h_1}W_{h_2} - \sigma(h_1,h_2)W_{h_1h_2}) \end{aligned}$$

$$\begin{aligned} f'(W_1 - 1) &= 1 \otimes W_1 - 1 \otimes 1 \\ &= 1 \otimes (W_1 - 1) \end{aligned}$$

Como $\chi'(h) = \sigma(g,h)^{-1}\sigma(h,g)\chi(h)$, temos:

$$\begin{aligned}
f'(YW_h - \chi(h)W_hY) &= (1\otimes Y + x\otimes W_g)(h\otimes W_h) - \chi(h)(h\otimes W_h)(1\otimes Y + x\otimes W_g)\\
&= h\otimes YW_h + xh\otimes W_gW_h - \chi(h)h\otimes W_hY - \chi(h)hx\otimes W_hW_g\\
&= h\otimes (YW_h - \chi(h)W_hY) + \chi'(h)hx\otimes W_gW_h - \chi(h)hx\otimes W_hW_g\\
&= h\otimes (YW_h - \chi(h)W_hY) + \chi'(h)hx\otimes W_gW_h - \chi'(h)\sigma(g,h)hx\otimes W_{gh}\\
&\quad + \chi'(h)\sigma(g,h)hx\otimes W_{gh} - \chi(h)hx\otimes W_hW_g\\
&= h\otimes (YW_h - \chi(h)W_hY) + \chi'(h)hx\otimes (W_gW_h - \sigma(g,h)W_{gh})\\
&\quad + \chi(h)\sigma(h,g)hx\otimes W_{gh} - \chi(h)hx\otimes W_hW_g\\
&= h\otimes (YW_h - \chi(h)W_hY) + \chi'(h)hx\otimes (W_gW_h - \sigma(g,h)W_{gh})\\
&\quad - \chi(h)hx\otimes (W_hW_g - \sigma(h,g)W_{gh})
\end{aligned}$$

Como $\mu = -a\sigma(g,g)^{-1}\cdots\sigma(g,g^{d-1})^{-1}$, $\pi\colon \mathcal{L}(\mathbb{G}) \to A_{\sigma,a}(\mathbb{G})$ é morfismo de álgebras e $\ker\pi = \mathcal{I}_{\sigma,a}(\mathbb{G})$, temos que:

$$\begin{aligned}
(A(\mathbb{G})\otimes\pi)\circ f'(Y^d - aW_{g^d}) &= (A(\mathbb{G})\otimes\pi)\big((1\otimes Y + x\otimes W_g)^d - ag^d\otimes W_{g^d}\big)\\
&= (1\otimes X + x\otimes T_g)^d - ag^d\otimes T_{g^d}\\
&\overset{\text{Corolário A.8}}{=} 1\otimes X^d + x^d\otimes (T_g)^d - ag^d\otimes T_{g^d}\\
&= a1\otimes T_{g^d} + \mu(1-g^d)\otimes (T_g)^d - ag^d\otimes T_{g^d}\\
&= a(1-g^d)\otimes T_{g^d} + \mu\sigma(g,g)\cdots\sigma(g,g^{d-1})(1-g^d)\otimes T_{g^d}\\
&= 0
\end{aligned}$$

implica $f'(Y^d - aW_{g^d}) \in A(\mathbb{G})\otimes\mathcal{I}_{\sigma,a}(\mathbb{G})$.

Pelo Corolário 1.14, $A_{\sigma,a}(\mathbb{G})$ é $A(\mathbb{G})$-comódulo álgebra com coação dada por:

$$\begin{aligned}
\beta\colon A_{\sigma,a}(\mathbb{G}) &\longrightarrow A(\mathbb{G})\otimes A_{\sigma,a}(\mathbb{G})\\
X &\longmapsto 1\otimes X + x\otimes T_g\\
T_h &\longmapsto h\otimes T_h,\ \forall h\in G
\end{aligned}$$

Vejamos que $A_{\sigma,a}(\mathbb{G})$ é $A(\mathbb{G})$-bicomódulo. De fato, como $\{T_hX^i;\ h\in G, 0\le i\le d-1\}$ é base linear de $A_{\sigma,a}(\mathbb{G})$, precisamos verificar apenas para os elementos da base. Sejam $h\in G$ e $0\le i\le d-1$. Como ρ e β são morfismos de álgebras, temos:

$$\begin{aligned}
(A(\mathbb{G})\otimes\rho)\circ\beta(T_hX^i) &= (A(\mathbb{G})\otimes\rho)\big((h\otimes T_h)(1\otimes X + x\otimes T_g)^i\big)\\
&= (h\otimes T_h\otimes h)(1\otimes(1\otimes x + X\otimes g) + x\otimes T_g\otimes g)^i\\
&= (h\otimes T_h\otimes h)(1\otimes 1\otimes x + 1\otimes X\otimes g + x\otimes T_g\otimes g)^i\\
&= (\beta\otimes A(\mathbb{G}))\big((T_h\otimes h)(1\otimes x + X\otimes g)^i\big)\\
&= (\beta\otimes A(\mathbb{G}))\circ\rho(T_hX^i)
\end{aligned}$$

Portanto $A_{\sigma,a}(\mathbb{G})$ é $A(\mathbb{G})$-bicomódulo.

Vejamos agora que $A_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois à esquerda, ou seja, que:

$$\kappa_l\colon A_{\sigma,a}(\mathbb{G})\otimes A_{\sigma,a}(\mathbb{G}) \to A(\mathbb{G})\otimes A_{\sigma,a}(\mathbb{G})$$

é bijetor. De fato, para cada $h\in G$ temos:

$$\begin{aligned}
\kappa_l(T_h\otimes 1) &= \beta(T_h)1\\
&= h\otimes T_h
\end{aligned}$$

e pela $A_{\sigma,a}(\mathbb{G})$-linearidade à direita temos:

$$\begin{aligned}\kappa_l(\sigma(h,h^{-1})^{-1}T_h\otimes T_{h^{-1}}) &= \sigma(h,h^{-1})^{-1}\kappa_l(T_h\otimes 1)T_{h^{-1}}\\ &= \sigma(h,h^{-1})^{-1}(h\otimes T_h)T_{h^{-1}}\\ &= \sigma(h,h^{-1})^{-1}\sigma(h,h^{-1})h\otimes T_{hh^{-1}}\\ &= h\otimes 1\end{aligned}$$

Assuma que $hx^t\otimes 1$ está na imagem de κ_l, $\forall h\in G$ e $0\leq t\leq i-1$.
Seja $\eta_{h,t}\in A_{\sigma,a}(\mathbb{G})\otimes A_{\sigma,a}(\mathbb{G})$ um elemento tal que $\kappa_l(\eta_{h,t})=hx^t\otimes 1$. Então:

$$\begin{aligned}\kappa_l(X^i\eta_{h,0}) &= \kappa_l(\sigma(h,h^{-1})^{-1}X^iT_h\otimes T_{h^{-1}})\\ &= \sigma(h,h^{-1})^{-1}\beta(X^i)\beta(T_h)T_{h^{-1}}\\ &= \sigma(h,h^{-1})^{-1}(1\otimes X+x\otimes T_g)^i(h\otimes T_h)T_{h^{-1}}\\ &= (1\otimes X+x\otimes T_g)^i(h\otimes 1)\\ &\overset{\text{Proposição A.7}}{=} \sum_{t=0}^{i}\binom{i}{t}_q (x\otimes T_g)^{i-t}(1\otimes X)^t(h\otimes 1)\\ &= \sum_{t=0}^{i}\binom{i}{t}_q x^{i-t}h\otimes (T_g)^{i-t}X^t\\ &= \sum_{t=0}^{i}\binom{i}{t}_q \chi(h)^{i-t}hx^{i-t}\otimes (T_g)^{i-t}X^t\\ &= \chi(h)^ihx^i\otimes (T_g)^i+\sum_{t=1}^{i}\binom{i}{t}_q \chi(h)^{i-t}hx^{i-t}\otimes (T_g)^{i-t}X^t\\ &= \chi(h)^ihx^i\otimes (T_g)^i+\sum_{t=1}^{i}\binom{i}{t}_q \chi(h)^{i-t}\kappa_l(\eta_{h,i-t})(T_g)^{i-t}X^t\end{aligned}$$

Portanto temos que:

$$\kappa_l\Big(\chi(h)^{-i}\Big(X^i\eta_{h,0}-\sum_{t=1}^{i}\binom{i}{t}_q\chi(h)^{i-t}\eta_{h,i-t}(T_g)^{i-t}X^t\Big)(T_g)^{-i}\Big)=hx^i\otimes 1$$

Logo, todos os elementos da forma $hx^i\otimes 1$ estão na imagem de κ_l. Como κ_l é $A_{\sigma,a}(\mathbb{G})$-linear à direita, temos que κ_l é sobrejetora.

Assim, temos que $\dim A_{\sigma,a}(\mathbb{G})\otimes A_{\sigma,a}(\mathbb{G})\geq \dim A(\mathbb{G})\otimes A_{\sigma,a}(\mathbb{G})$. Como $A_{\sigma,a}(\mathbb{G})$ é algebra não-nula, $\dim A_{\sigma,a}(\mathbb{G})\neq 0$. Portanto $\dim A_{\sigma,a}(\mathbb{G})\geq \dim A(\mathbb{G})$.

Pelo Lema 2.14, temos que $\dim A_{\sigma,a}(\mathbb{G})\leq |G|d$ e sabemos que $\dim A(\mathbb{G})=|G|d$. Logo $\dim A_{\sigma,a}(\mathbb{G})\otimes A_{\sigma,a}(\mathbb{G})=\dim A(\mathbb{G})\otimes A_{\sigma,a}(\mathbb{G})$ e κ_l é isomorfismo, o que implica que $A_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois. □

Lema 3.14. *Sejam $\mathbb{G}=(G,g,\chi)$ e $\mathbb{G}'=(G,g,\chi',\mu)$ dois conjuntos de dados de grupo com $\chi'(h)=\sigma(g,h)^{-1}\sigma(h,g)\chi(h)$, $\forall h\in G$. As álgebras de Hopf $A(\mathbb{G}')$ e $A(\mathbb{G})$ são isomorfas se, e somente se, $\mu=0$ e existe $u\in Aut_g(G)$ tal que:*

$$\chi\circ u(h)=\sigma(g,h)^{-1}\sigma(h,g)\chi(h),\ \forall h\in G$$

Demonstração. As álgebras de Hopf $A(\mathbb{G}')$ e $A(\mathbb{G})$ são isomorfas se, e somente se, $\mathbb{G}$ e $\mathbb{G}'$ são isomorfos. Mas pela Definição 2.2, $\mathbb{G}$ e $\mathbb{G}'$ são isomorfos se, e somente se, $\mu=0$ e existe $u\in \mathrm{Aut}_g(G)$ tal que $\chi\circ u=\chi'$. A equação $\chi\circ u=\chi'$ é equivalente a:

$$\chi\circ u(h)=\sigma(g,h)^{-1}\sigma(h,g)\chi(h),\ \forall h\in G$$

□

3.5 Descrição dos objetos $A(\mathbb{G})$-biGalois com $\mathbb{G}$ do tipo III e IV

Proposição 3.15. *Seja $\mathbb{G} = (G, g, \chi)$ um conjunto de dados de grupo do tipo III. Então temos um isomorfismo de grupos:*

$$BiGal(A(\mathbb{G})) \cong \Gamma(\mathbb{G})$$

Demonstração. Considere a função:

$$\begin{aligned} \Psi\colon \Gamma(\mathbb{G}) &\longrightarrow \mathrm{BiGal}(A(\mathbb{G})) \\ (u, \overline{\sigma}) &\longmapsto \left[A^u_{\sigma,0}(\mathbb{G})\right] \end{aligned}$$

Pela Proposição 3.3, temos que $A^u_{\sigma,0}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois para todo $(u, \overline{\sigma}) \in \Gamma(\mathbb{G})$. Logo, a função Ψ está bem definida.

Pela Proposição 3.4, a função Ψ é injetora.

Pela Proposição 3.5, a função Ψ é morfismo de grupos.

Precisamos verificar que Ψ é sobrejetora. Seja Z um objeto $A(\mathbb{G})$-biGalois. Em particular, Z é um objeto $A(\mathbb{G})$-Galois à direita e, pela Proposição 2.27, existem $\sigma \in Z^2(G, \mathbb{K}^*)$ e $a \in \mathbb{K}$ tais que $Z = A_{\sigma,a}(\mathbb{G})$ como $A(\mathbb{G})$-comódulo álgebras à direita.

Tome $\mathbb{G}' = (G, g, \chi', \mu)$ com:

$$\begin{aligned} \chi'(h) &= \sigma(g,h)^{-1}\sigma(h,g)\chi(h), \; \forall h \in G \\ \mu &= -a\sigma(g,g)^{-1} \cdots \sigma(g, g^{d-1})^{-1} \end{aligned}$$

Pela Proposição 3.13, temos que $A_{\sigma,a}(\mathbb{G})$ é objeto $A(\mathbb{G}')$-$A(\mathbb{G})$-biGalois. Como Z é objeto $A(\mathbb{G})$-biGalois, pelo Teorema 1.83, temos que $A(\mathbb{G}') \cong A(\mathbb{G})$. Se $a \neq 0$, teríamos que $\mathbb{G}'$ seria um conjunto de dados de grupo do tipo VI, o que impossibilitaria o isomorfismo. Portanto $a = 0$.

Pelo Lema 3.14, existe $u \in \mathrm{Aut}_g(G)$ tal que $(u, \overline{\sigma}) \in \Gamma(\mathbb{G})$. Pela Proposição 3.3, temos que $A^u_{\sigma,0}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois.

Pelo Teorema 1.83, existe $f \in \mathrm{Aut}_{Hopf}(A(\mathbb{G}))$ tal que, se β é a coação à esquerda de Z e β_u é a coação à esquerda de $A^u_{\sigma,0}(\mathbb{G})$, então $\beta = (f \otimes Z) \circ \beta_u$. Diremos que $Z = {}^f A^u_{\sigma,0}(\mathbb{G})$.

Pela Proposição 2.10, existem $v \in \mathrm{Aut}_{g,\chi}(G)$ e $r \in \mathbb{K}^*$ tais que $f(x) = rx$ e $f(h) = v(h)$, $\forall h \in G$. Considere uma função $\theta\colon G \to \mathbb{K}^*$ com $\theta(1) = 1$ e $\theta(g) = r$.

Claramente $A_{\partial(\theta)\sigma,0}(\mathbb{G})$ é objeto $A(\mathbb{G})$-Galois.

Como g é central, temos que:

$$\begin{aligned} \partial(\theta)(g,h) &= \theta(h)\theta(gh)^{-1}\theta(g) \\ &= \theta(g)\theta(hg)^{-1}\theta(h) \\ &= \partial(\theta)(h,g) \end{aligned}$$

Como $u \in \mathrm{Aut}_g(G)$ e $v \in \mathrm{Aut}_{g,\chi}(G) \subset \mathrm{Aut}_g(G)$, temos que $v \circ u \in \mathrm{Aut}_g(G)$. Além disso, temos que:

$$\begin{aligned} \chi \circ v \circ u(h) &= \chi \circ u(h) \\ &= \sigma(g,h)^{-1}\sigma(h,g)\chi(h) \\ &= \sigma(g,h)^{-1}\partial(\theta)(g,h)^{-1}\partial(\theta)(g,h)\sigma(h,g)\chi(h) \\ &= \sigma(g,h)^{-1}\partial(\theta)(g,h)^{-1}\partial(\theta)(h,g)\sigma(h,g)\chi(h) \end{aligned}$$

Logo, $(v \circ u, \overline{\partial(\theta)\sigma}) \in \Gamma(\mathbb{G})$ e $A^{v\circ u}_{\partial(\theta)\sigma,0}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois.

Considere a função:

$$\begin{aligned} \phi\colon \mathcal{V}(\mathbb{G}) &\longrightarrow {}^{f}A^{u}_{\sigma,0}(\mathbb{G}) \\ Y &\longmapsto X \\ W_h &\longmapsto \theta(h)T_h \end{aligned}$$

onde $\mathcal{V}(\mathbb{G})$ é $A(\mathbb{G})$-bicomódulo com estrutura à direita dada por:

$$\begin{aligned} \rho_{\mathcal{V}(\mathbb{G})}\colon \mathcal{V}(\mathbb{G}) &\longrightarrow \mathcal{V}(\mathbb{G}) \otimes A(\mathbb{G}) \\ Y &\longmapsto 1 \otimes x + Y \otimes g \\ W_h &\longmapsto W_h \otimes h \end{aligned}$$

e estrutura à esquerda dada por:

$$\begin{aligned} \beta_{\mathcal{V}(\mathbb{G})}\colon \mathcal{V}(\mathbb{G}) &\longrightarrow A(\mathbb{G}) \otimes \mathcal{V}(\mathbb{G}) \\ Y &\longmapsto 1 \otimes Y + x \otimes T_g \\ W_h &\longmapsto v \circ u(h) \otimes W_h \end{aligned}$$

Vejamos que ϕ é morfismo de $A(\mathbb{G})$-comódulos à direita:

$$\begin{aligned} \rho \circ \phi(Y) &= \rho(X) \\ &= 1 \otimes x + X \otimes g \\ &= (\phi \otimes A(\mathbb{G}))(1 \otimes x + Y \otimes g) \\ &= (\phi \otimes A(\mathbb{G})) \circ \rho_{\mathcal{V}(\mathbb{G})}(Y) \end{aligned}$$

e para cada $h \in G$:

$$\begin{aligned} \rho \circ \phi(W_h) &= \rho(\theta(h)T_h) \\ &= \theta(h)T_h \otimes h \\ &= (\phi \otimes A(\mathbb{G}))(W_h \otimes h) \\ &= (\phi \otimes A(\mathbb{G})) \circ \rho_{\mathcal{V}(\mathbb{G})}(W_h) \end{aligned}$$

Vejamos que ϕ é morfismo de $A(\mathbb{G})$-comódulos à esquerda:

$$\begin{aligned} \beta \circ \phi(Y) &= (f \otimes Z) \circ \beta_u(X) \\ &= (f \otimes Z)(1 \otimes X + x \otimes T_g) \\ &= f(1) \otimes X + f(x) \otimes T_g \\ &= 1 \otimes X + rx \otimes T_g \\ &= 1 \otimes X + \theta(g)x \otimes T_g \\ &= (A(\mathbb{G}) \otimes \phi)(1 \otimes Y + x \otimes W_g) \\ &= (A(\mathbb{G}) \otimes \phi) \circ \beta_{\mathcal{V}(\mathbb{G})}(Y) \end{aligned}$$

e para cada $h \in G$:

$$\begin{aligned} \beta \circ \phi(W_h) &= (f \otimes Z) \circ \beta_u(\theta(h)T_h) \\ &= (f \otimes Z)(\theta(h)u(h) \otimes T_h) \\ &= \theta(h)f(u(h)) \otimes T_h \\ &= \theta(h)v \circ u(h) \otimes T_h \\ &= (A(\mathbb{G}) \otimes \phi)(v \circ u(h) \otimes W_h) \\ &= (A(\mathbb{G}) \otimes \phi) \circ \beta_{\mathcal{V}(\mathbb{G})}(W_h) \end{aligned}$$

Portanto ϕ é morfismo de $A(\mathbb{G})$-bicomódulos.

Pela Proposição 1.19, temos um morfismo de $A(\mathbb{G})$-bicomódulo álgebras:

$$\begin{aligned} \phi' \colon \mathcal{L}(\mathbb{G}) &\longrightarrow {}^{f}A^{u}_{\sigma,0}(\mathbb{G}) \\ Y &\longmapsto X \\ W_h &\longmapsto \theta(h)T_h \end{aligned}$$

Durante a demonstração da Proposição 2.15, mostramos que $\mathcal{I}_{\partial(\theta)\sigma,0}(\mathbb{G})$ é $A(\mathbb{G})$-subcomódulo à direita de $\mathcal{L}(\mathbb{G})$.

Durante a demonstração da Proposição 3.3, mostramos que, se $v \circ u \in \mathrm{Aut}_g(G)$ satisfaz a condição:

$$\chi \circ (v \circ u)(h) = (\partial(\theta)\sigma)(g,h)^{-1}(\partial(\theta)\sigma)(h,g)\chi(h), \ \forall h \in G$$

então $\mathcal{I}_{\partial(\theta)\sigma,0}(\mathbb{G})$ é $A(\mathbb{G})$-subcomódulo à esquerda de $\mathcal{L}(\mathbb{G})$.

Pelo Corolário 1.21, temos um morfismo de $A(\mathbb{G})$-bicomódulo álgebras:

$$\begin{aligned} F \colon A^{v\circ u}_{\partial(\theta)\sigma,0}(\mathbb{G}) &\longrightarrow {}^{f}A^{u}_{\sigma,0}(\mathbb{G}) \\ X &\longmapsto X \\ T_h &\longmapsto \theta(h)T_h \end{aligned}$$

Como $A^{v\circ u}_{\partial(\theta)\sigma,0}(\mathbb{G})$ e ${}^{f}A^{u}_{\sigma,0}(\mathbb{G})$ são objetos $A(\mathbb{G})$-biGalois, segue que F é isomorfismo e $\left[A^{v\circ u}_{\partial(\theta)\sigma,0}(\mathbb{G})\right] = [Z]$. Portanto Ψ é sobrejetora. □

Proposição 3.16. *Seja $\mathbb{G} = (G, g, \chi)$ um conjunto de dados de grupo do tipo IV. Então temos um isomorfismo de grupos:*

$$\mathit{BiGal}(A(\mathbb{G})) \cong \Gamma(\mathbb{G})$$

Demonstração. Considere a função:

$$\begin{aligned} \Psi \colon \Gamma(\mathbb{G}) &\longrightarrow \mathrm{BiGal}(A(\mathbb{G})) \\ (u, \overline{\sigma}) &\longmapsto \left[A^{u}_{\sigma,0}(\mathbb{G})\right] \end{aligned}$$

Pela Proposição 3.3, temos que $A^{u}_{\sigma,0}(\mathbb{G})$ é objeto $A(\mathbb{G})$-biGalois para todo $(u, \overline{\sigma}) \in \Gamma(\mathbb{G})$. Logo, a função Ψ está bem definida.

Pela Proposição 3.4, a função Ψ é injetora.

Pela Proposição 3.5, a função Ψ é morfismo de grupos.

A verificação de que Ψ é sobrejetora é feita do mesmo modo que no tipo III, com a diferença de que no tipo IV não há possibilidade de $a \neq 0$ pois, pela Proposição 2.28, quando $\mathbb{G}$ é do tipo IV, os objetos $A(\mathbb{G})$-Galois à direita são da forma $A_{\sigma,0}(\mathbb{G})$. □

3.6 Descrição dos objetos $A(\mathbb{G})$-biGalois com $\mathbb{G}$ do tipo V e VI

Proposição 3.17. *Seja $\mathbb{G} = (G, g, \chi)$ um conjunto de dados de grupo do tipo V. Então temos um isomorfismo de grupos:*

$$\mathit{BiGal}(A(\mathbb{G})) \cong \Gamma(\mathbb{G})$$

Demonstração. Seja $\sigma \in Z^2(G, \mathbb{K}^*)$ tal que $\chi(h)^d = \sigma(g^d, h)\sigma(h, g^d)^{-1}$. Tome $\mathbb{G}_\sigma = (G, g, \chi_\sigma)$ onde $\chi_\sigma \colon G \to \mathbb{K}^*$ é dado por $\chi_\sigma(h) = \sigma(g,h)^{-1}\sigma(h,g)\chi(h)$.

Como $(\sigma(g,h)^{-1}\sigma(h,g))^d = \sigma(g^d,h)^{-1}\sigma(h,g^d)$, temos que $\chi^d_\sigma(h) = 1$ e $\mathbb{G}_\sigma$ é um conjunto de dados de grupo do tipo III.

Considere agora $\sigma^{-1} \in Z^2(G, \mathbb{K}^*)$. Temos que $A_{\sigma^{-1},0}(\mathbb{G})$ é um objeto $A(\mathbb{G}_\sigma)$-Galois á direita.

Tomando $\mathbb{G}' = (G, g, \chi')$ com $\chi' \colon G \to \mathbb{K}^*$ dado por:

$$\chi'(h) = (\sigma^{-1})(g,h)^{-1}(\sigma^{-1})(h,g)\chi_\sigma(h)$$

pela Proposição 3.13, temos que $A_{\sigma^{-1},0}(\mathbb{G})$ é um objeto $A(\mathbb{G}')$-$A(\mathbb{G}_\sigma)$-biGalois. Mas para cada $h \in G$:

$$\begin{aligned}
\chi'(h) &= (\sigma^{-1})(g,h)^{-1}(\sigma^{-1})(h,g)\chi_\sigma(h) \\
&= (\sigma^{-1})(g,h)^{-1}(\sigma^{-1})(h,g)\sigma(g,h)^{-1}\sigma(h,g)\chi(h) \\
&= \chi(h)
\end{aligned}$$

Portanto $\mathbb{G}' = \mathbb{G}$. Pela Proposição 1.84, temos um isomorfismo de grupos:

$$\mathrm{BiGal}(A(\mathbb{G})) \cong \mathrm{BiGal}(A(\mathbb{G}_\sigma))$$

Pela Proposição 3.15, temos um isomorfismo de grupos:

$$\mathrm{BiGal}(A(\mathbb{G}_\sigma) \cong \Gamma(\mathbb{G}_\sigma)$$

Observe que, se $(u, \overline{\tau}) \in \Gamma(\mathbb{G}_\sigma)$, então:

$$\chi_\sigma \circ u(h) = \tau(g,h)^{-1}\tau(h,g)\chi_\sigma(h)$$

Esta equação nos permite calcular $\chi \circ u(h)$:

$$\begin{aligned}
\chi \circ u(h) &= \sigma(g, u(h))\sigma(u(h), g)^{-1}\chi_\sigma(u(h)) \\
&= (u \cdot \sigma)(g,h)(u \cdot \sigma)(h,g)^{-1}\tau(g,h)^{-1}\tau(h,g)\chi_\sigma(h) \\
&= (u \cdot \sigma)(g,h)(u \cdot \sigma)(h,g)^{-1}\tau(g,h)^{-1}\tau(h,g)\sigma(g,h)^{-1}\sigma(h,g)\chi(h) \\
&= ((u \cdot \sigma)(g,h)^{-1})^{-1}(u \cdot \sigma)(h,g)^{-1}\tau(g,h)^{-1}\tau(h,g)\sigma(g,h)^{-1}\sigma(h,g)\chi(h)
\end{aligned}$$

Logo $(u, \overline{(u \cdot \sigma)^{-1}\sigma\tau}) \in \Gamma(\mathbb{G})$ e podemos considerar a seguinte função:

$$\begin{aligned}
\varphi \colon \Gamma(\mathbb{G}_\sigma) &\longrightarrow \Gamma(\mathbb{G}) \\
(u, \overline{\tau}) &\longmapsto (u, \overline{(u \cdot \sigma)^{-1}\sigma\tau})
\end{aligned}$$

Vejamos que φ é morfismo de grupos. De fato, dados $(u_1, \overline{\tau_1}), (u_2, \overline{\tau_2}) \in \Gamma(\mathbb{G}_\sigma)$, temos:

$$\begin{aligned}
\varphi\big((u_1, \overline{\tau_1})\big)\varphi\big((u_2, \overline{\tau_2})\big) &= (u_1, \overline{(u_1 \cdot \sigma)^{-1}\sigma\tau_1})(u_2, \overline{(u_2 \cdot \sigma)^{-1}\sigma\tau_2}) \\
&= (u_1 \circ u_2, \overline{(u_2 \cdot ((u_1 \cdot \sigma)^{-1}\sigma\tau_1))((u_2 \cdot \sigma)^{-1}\sigma\tau_2)}) \\
&= (u_1 \circ u_2, \overline{(u_2 \cdot (u_1 \cdot \sigma)^{-1})(u_2 \cdot \sigma)(u_2 \cdot \tau_1)(u_2 \cdot \sigma)^{-1}\sigma\tau_2}) \\
&= (u_1 \circ u_2, \overline{((u_1 \circ u_2) \cdot \sigma)^{-1}(u_2 \cdot \tau_1)\sigma\tau_2}) \\
&= \varphi\big((u_1 \circ u_2, \overline{(u_2 \cdot \tau_1)\tau_2})\big) \\
&= \varphi\big((u_1, \overline{\tau_1})(u_2, \overline{\tau_2})\big)
\end{aligned}$$

Vejamos que φ é injetor. De fato, se $(u_1, \overline{\tau_1}), (u_2, \overline{\tau_2}) \in \Gamma(\mathbb{G}_\sigma)$ são tais que:

$$\varphi\big((u_1, \overline{\tau_1})\big) = \varphi\big((u_2, \overline{\tau_2})\big)$$

então:

$$(u_1, \overline{(u_1 \cdot \sigma)^{-1}\sigma\tau_1}) = (u_2, \overline{(u_2 \cdot \sigma)^{-1}\sigma\tau_2})$$

o que implica que $u_1 = u_2 = u$ e existe $\theta \in B^2(G, \mathbb{K}^*)$ tal que:

$$(u \cdot \sigma)^{-1}\sigma\tau_1\big((u \cdot \sigma)^{-1}\sigma\tau_2\big)^{-1} = \partial(\theta)$$

Logo, temos que:

$$\tau_1\tau_2^{-1} = \partial(\theta)$$

ou seja, $\overline{\tau_1} = \overline{\tau_2}$ e φ é injetor.

Vejamos que φ é sobrejetor. De fato, seja $(u, \overline{\tau}) \in \Gamma(\mathbb{G})$. Temos que:

$$\begin{aligned}
\chi_\sigma \circ u(h) &= \sigma(g, u(h))^{-1}\sigma(u(h), g)\chi(u(h)) \\
&= (u \cdot \sigma)(g, h)^{-1}(u \cdot \sigma)(h, g)\chi(u(h)) \\
&= (u \cdot \sigma)(g, h)^{-1}(u \cdot \sigma)(h, g)\tau(g, h)^{-1}\tau(h, g)\chi(h) \\
&= (u \cdot \sigma)(g, h)^{-1}(u \cdot \sigma)(h, g)\tau(g, h)^{-1}\tau(h, g)\sigma(g, h)\sigma(h, g)^{-1}\chi_\sigma(h)
\end{aligned}$$

o que implica que $(u, \overline{(u \cdot \sigma)\sigma^{-1}\tau}) \in \Gamma(\mathbb{G}_\sigma)$. Note que:

$$\begin{aligned}
\varphi\big((u, \overline{(u \cdot \sigma)\sigma^{-1}\tau})\big) &= (u, \overline{(u \cdot \sigma)^{-1}\sigma(u \cdot \sigma)\sigma^{-1}\tau}) \\
&= (u, \overline{\tau})
\end{aligned}$$

Portanto φ é um isomorfismo de grupos. Assim temos os seguintes isomorfismos de grupos:

$$\mathrm{BiGal}(A(\mathbb{G})) \cong \mathrm{BiGal}(A(\mathbb{G}_\sigma)) \cong \Gamma(\mathbb{G}_\sigma) \cong \Gamma(\mathbb{G})$$

Logo, temos um isomorfismo de grupos:

$$\mathrm{BiGal}(A(\mathbb{G})) \cong \Gamma(\mathbb{G})$$

$\square$

Proposição 3.18. *Seja $\mathbb{G} = (G, g, \chi, \mu)$ um conjunto de dados de grupo do tipo VI. Então temos um isomorfismo de grupos:*

$$\mathit{BiGal}(A(\mathbb{G})) \cong \Gamma(\mathbb{G})$$

e

$$\mathit{Gal}\big(A(\mathbb{G})\big) \cong H^2(G, \mathbb{K}^*) \coprod H^2_{g^d, g^d}(G, \mathbb{K}^*)$$

Demonstração. Tome $\mathbb{G}_{red} = (G, g, \chi)$. Como $d = o(\chi(g)) < o(g)$ e $\chi^d = 1$, temos que $\mathbb{G}_{red}$ é um conjunto de dados de grupo do tipo III.

Considere agora $\sigma \in Z^2(G, \mathbb{K}^*)$ dado por $\sigma(h_1, h_2) = 1$, $\forall h_1, h_2 \in G$. Para qualquer $a \in \mathbb{K}$ a equação (2.4.1) é satisfeita. Logo $A_{\sigma,-\mu}(\mathbb{G}_{red})$ é um objeto $A(\mathbb{G}_{red})$-Galois á direita. Tomando $\mathbb{G}' = (G, g, \chi', \mu')$ com $\chi' \colon G \to \mathbb{K}^*$ dado por:

$$\chi'(h) = \sigma(g, h)^{-1}\sigma(h, g)\chi(h) = \chi(h)$$

e $\mu' \in \mathbb{K}$ dado por:

$$\mu' = -(-\mu)\sigma(g, g)^{-1} \cdots \sigma(g, g^{d-1})^{-1} = \mu$$

pela Proposição 3.13, temos que $A_{\sigma,-\mu}(\mathbb{G}_{red})$ é um objeto $A(\mathbb{G}')$-$A(\mathbb{G}_{red})$-biGalois. Mas claramente $\mathbb{G}' = \mathbb{G}$. Pela Proposição 1.84, temos uma bijeção:

$$\mathrm{Gal}\big(A(\mathbb{G})\big) \cong \mathrm{Gal}\big(A(\mathbb{G}_{red})\big)$$

e um isomorfismo de grupos:

$$\mathrm{BiGal}(A(\mathbb{G})) \cong \mathrm{BiGal}(A(\mathbb{G}_{red}))$$

Pela Proposição 2.27, temos uma bijeção:

$$\mathrm{Gal}\big(A(\mathbb{G}_{red})\big) \cong H^2(G,\mathbb{K}^*) \coprod H^2_{g^d,g^d}(G,\mathbb{K}^*)$$

Pela Proposição 3.15, temos um isomorfismo de grupos:

$$\mathrm{BiGal}(A(\mathbb{G}_{red}) \cong \Gamma(\mathbb{G}_{red})$$

Observe que, se $(u,\overline{\tau}) \in \Gamma(\mathbb{G}_{red})$, então:

$$\begin{aligned}
\chi \circ u(h) &= \sigma(g,u(h))\sigma(u(h),g)^{-1}\chi_\sigma(u(h)) \\
&= (u\cdot\sigma)(g,h)(u\cdot\sigma)(h,g)^{-1}\tau(g,h)^{-1}\tau(h,g)\chi_\sigma(h) \\
&= (u\cdot\sigma)(g,h)(u\cdot\sigma)(h,g)^{-1}\tau(g,h)^{-1}\tau(h,g)\sigma(g,h)^{-1}\sigma(h,g)\chi(h) \\
&= ((u\cdot\sigma)(g,h)^{-1})^{-1}(u\cdot\sigma)(h,g)^{-1}\tau(g,h)^{-1}\tau(h,g)\sigma(g,h)^{-1}\sigma(h,g)\chi(h)
\end{aligned}$$

Logo $(u,\overline{(u\cdot\sigma)^{-1}\sigma\tau}) \in \Gamma(\mathbb{G})$ e podemos considerar a seguinte função:

$$\begin{aligned}
\varphi\colon \Gamma(\mathbb{G}_{red}) &\longrightarrow \Gamma(\mathbb{G}) \\
(u,\overline{\tau}) &\longmapsto (u,\overline{(u\cdot\sigma)^{-1}\sigma\tau})
\end{aligned}$$

Vejamos que φ é morfismo de grupos. De fato, dados $(u_1,\overline{\tau_1}),(u_2,\overline{\tau_2}) \in \Gamma(\mathbb{G}_{red})$, temos:

$$\begin{aligned}
\varphi\big((u_1,\overline{\tau_1})\big)\varphi\big((u_2,\overline{\tau_2})\big) &= (u_1,\overline{(u_1\cdot\sigma)^{-1}\sigma\tau_1})(u_2,\overline{(u_2\cdot\sigma)^{-1}\sigma\tau_2}) \\
&= (u_1\circ u_2,\overline{(u_2\cdot((u_1\cdot\sigma)^{-1}\sigma\tau_1))((u_2\cdot\sigma)^{-1}\sigma\tau_2)}) \\
&= (u_1\circ u_2,\overline{(u_2\cdot(u_1\cdot\sigma)^{-1})(u_2\cdot\sigma)(u_2\cdot\tau_1)(u_2\cdot\sigma)^{-1}\sigma\tau_2}) \\
&= (u_1\circ u_2,\overline{((u_1\circ u_2)\cdot\sigma)^{-1}(u_2\cdot\tau_1)\sigma\tau_2}) \\
&= \varphi\big((u_1\circ u_2,\overline{(u_2\cdot\tau_1)\tau_2})\big) \\
&= \varphi\big((u_1,\overline{\tau_1})(u_2,\overline{\tau_2})\big)
\end{aligned}$$

Vejamos que φ é injetor. De fato, se $(u_1,\overline{\tau_1}),(u_2,\overline{\tau_2}) \in \Gamma(\mathbb{G}_{red})$ são tais que:

$$\varphi\big((u_1,\overline{\tau_1})\big) = \varphi\big((u_2,\overline{\tau_2})\big)$$

então:

$$(u_1,\overline{(u_1\cdot\sigma)^{-1}\sigma\tau_1}) = (u_2,\overline{(u_2\cdot\sigma)^{-1}\sigma\tau_2})$$

o que implica que $u_1 = u_2$ e

Vejamos que φ é sobrejetor. De fato, seja $(u,\tau) \in \Gamma(\mathbb{G})$. Temos que:

$$\begin{aligned}
\chi_\sigma \circ u(h) &= \sigma(g,u(h))^{-1}\sigma(u(h),g)\chi(u(h)) \\
&= (u\cdot\sigma)(g,h)^{-1}(u\cdot\sigma)(h,g)\chi(u(h)) \\
&= (u\cdot\sigma)(g,h)^{-1}(u\cdot\sigma)(h,g)\tau(g,h)^{-1}\tau(h,g)\chi(h) \\
&= (u\cdot\sigma)(g,h)^{-1}(u\cdot\sigma)(h,g)\tau(g,h)^{-1}\tau(h,g)\sigma(g,h)\sigma(h,g)^{-1}\chi_\sigma(h)
\end{aligned}$$

o que implica que $(u,\overline{(u\cdot\sigma)\sigma^{-1}\tau}) \in \Gamma(\mathbb{G}_{red})$. Note que:

$$\begin{aligned}
\varphi\big((u,\overline{(u\cdot\sigma)\sigma^{-1}\tau})\big) &= (u,\overline{(u\cdot\sigma)^{-1}\sigma(u\cdot\sigma)\sigma^{-1}\tau}) \\
&= (u,\overline{\tau})
\end{aligned}$$

Portanto φ é um isomorfismo de grupos. Assim temos os seguintes isomorfismos de grupos:

$$\mathrm{BiGal}(A(\mathbb{G})) \cong \mathrm{BiGal}(A(\mathbb{G}_{red})) \cong \Gamma(\mathbb{G}_{red}) \cong \Gamma(\mathbb{G})$$

Logo, temos um isomorfismo de grupos:

$$\mathrm{BiGal}(A(\mathbb{G})) \cong \Gamma(\mathbb{G})$$

$\square$

APÊNDICE

A. Q-CÁLCULO

Nesta seção apresentamos o Coeficiente Binomial Gaussiano, que é particularmente útil no cálculo de potências da forma $(a+b)^i$ quando estamos em uma álgebra não comutativa. Estes resultados se encontram em [13]. Fizemos uma pequena alteração na definição do coeficiente a fim de generalizá-lo para potências que a definição usual não cobre.

Observação A.1. *Seja $n \in \mathbb{N}$. Para cada $i \in \mathbb{N}$, chamaremos de s_i e r_i os números naturais tais que $i = s_i n + r_i$ com $0 \leq r_i < n$.*

Definição A.2. *Seja $q \in \mathbb{K}$. Definimos a função $\gamma\colon \mathbb{N} \to \mathbb{K}$ por $\gamma(i) = 1 + q + \cdots + q^{i-1}$ e denotaremos por i_q a imagem de i por γ.*

Lema A.3. *Se $q \in \mathbb{K}$ é uma n-ésima raíz primitiva da unidade, então para $i \in \mathbb{N}$ temos:*

$$i_q = (r_i)_q$$

Demonstração. Como q é uma n-ésima raíz primitiva da unidade, temos que $1 - q^n = 0$ e $1 - q \neq 0$. Logo, $n_q = 1 + q + \cdots + q^{n-1} = 0$, pois $1 - q^n = (1 - q)\left(1 + q + \cdots + q^{n-1}\right)$.

Assim, temos que:

$$\begin{aligned}
i_q &= 1 + q + \cdots + q^{i-1} \\
&= 1 + q + \cdots + q^{s_i n + r_i - 1} \\
&= \left(1 + q + \cdots + q^{n-1}\right) + q^n \left(1 + q + \cdots + q^{n-1}\right) + \cdots + \\
&\quad + q^{(s_i - 1)n} \left(1 + q + \cdots + q^{n-1}\right) + q^{s_i n} \left(1 + q + \cdots + q^{r_i - 1}\right) \\
&= (q^n)^{s_i} \left(1 + q + \cdots + q^{r_i - 1}\right) \\
&= (r_i)_q
\end{aligned}$$

$\square$

Definição A.4. *Seja q uma n-ésima raíz primitiva da unidade em $\mathbb{K}$. Para $i, j \in \mathbb{N}$ com $j \leq i$, definimos o coeficiente binomial Gaussiano como:*

$$\binom{i}{j}_q := \begin{cases} \dfrac{r_i!_q}{(r_i - r_j)!_q r_j!_q} & , \text{ se } r_i \geq r_j \\ 0 & , \text{ se } r_i < r_j \end{cases}$$

onde $l!_q := 1_q \cdots l_q$ e $0!_q := 1$.

Note que $\binom{i}{0}_q = 1 = \binom{i}{i}_q$, $\forall i \in \mathbb{N}$.

Proposição A.5. *A definição dada para o coeficiente binomial Gaussiano é equivalente à:*

$$\binom{i}{j}_q = \frac{i!_q}{(i-j)!_q j!_q}$$

se assumirmos que $\dfrac{n!_q}{n!_q} = 1$.

Demonstração. A convenção de que $\frac{n!_q}{n!_q} = 1$ é necessária para eliminar as indeterminações do tipo $\frac{0}{0}$.

Primeiramente note que $i!_q = (n!_q)^{s_i}\, r_i!_q$, pois:

$$\begin{aligned} i!_q &= 1_q \cdots i_q \\ &= (1_q \cdots n_q)\left((n+1)_q \cdots (2n)_q\right) \cdots \left(((s_i - 1)\,n + 1)_q \cdots (s_i n)_q\right)\left((s_i n + 1)_q \cdots i_q\right) \\ &\overset{\text{Lema A.3}}{=} \overbrace{(1_q \cdots n_q)\,(1_q \cdots n_q) \cdots (1_q \cdots n_q)}^{s_i\text{-vezes}} \left(1_q \cdots (r_i)_q\right) \\ &= (n!_q)^{s_i}\, r_i!_q \end{aligned}$$

Se $r_i \geq r_j$, temos:

$$\begin{aligned} \frac{i!_q}{(i-j)!_q j!_q} &= \frac{(n!_q)^{s_i}\, r_i!_q}{(n!_q)^{s_i - s_j}\,(r_i - r_j)!_q\,(n!_q)^{s_j}\, r_j!_q} \\ &= \left(\frac{n!_q}{n!_q}\right)^{s_i}\left(\frac{r_i!_q}{(r_i - r_j)!_q r_j!_q}\right) \\ &= \binom{i}{j}_q \end{aligned}$$

Se $r_i < r_j$, temos:

$$\begin{aligned} \frac{i!_q}{(i-j)!_q j!_q} &= \frac{(n!_q)^{s_i}\, r_i!_q}{(n!_q)^{s_i - s_j - 1}\,(n + r_i - r_j)!_q\,(n!_q)^{s_j}\, r_j!_q} \\ &= n!_q\left(\frac{n!_q}{n!_q}\right)^{s_i - 1}\left(\frac{r_i!_q}{(n + r_i - r_j)!_q r_j!_q}\right) \\ &= 0 \\ &= \binom{i}{j}_q \end{aligned}$$

Portanto, temos que:

$$\binom{i}{j}_q = \frac{i!_q}{(i-j)!_q j!_q}$$

□

Assumiremos que $\frac{n!_q}{n!_q} = 1$ e partir de agora, sempre que usarmos o coeficiente binomial Gaussiano, utilizaremos a expressão dada na proposição A.5.

Lema A.6. *Seja q uma n-ésima raíz primitiva da unidade em $\mathbb{K}$. Então para $i \geq 2$ e $1 \leq j \leq i - 1$ temos:*

$$\binom{i-1}{j}_q + \binom{i-1}{j-1}_q q^{i-j} = \binom{i}{j}_q$$

Demonstração. Temos que:

$$\begin{aligned}
\binom{i-1}{j}_q + \binom{i-1}{j-1}_q q^{i-j} &= \frac{(i-1)!_q}{(i-1-j)!_q j!_q} + \frac{(i-1)!_q q^{i-j}}{(i-j)!_q\,(j-1)!_q} \\
&= \frac{(i-1)!_q\,(i-j)_q + (i-1)!_q j_q q^{i-j}}{(i-j)!_q j!_q} \\
&= \frac{(i-1)!_q \left((i-j)_q + j_q q^{i-j}\right)}{(i-j)!_q j!_q} \\
&= \frac{(i-1)!_q \left(1+q+\cdots+q^{i-j-1} + \left(1+q+\cdots+q^{j-1}\right) q^{i-j}\right)}{(i-j)!_q j!_q} \\
&= \frac{(i-1)!_q \left(1+q+\cdots+q^{i-j-1} + q^{i-j} + q^{i-j+1} + \cdots + q^{i-1}\right)}{(i-j)!_q j!_q} \\
&= \frac{i!_q}{(i-j)!_q j!_q} \\
&= \binom{i}{j}_q
\end{aligned}$$

□

Proposição A.7. *Sejam A uma álgebra, q uma n-ésima raiz primitiva da unidade e $a, b \in A$ tais que $ba = qab$. Então para $0 \leq i \leq n$ temos que:*

$$(a+b)^i = \sum_{j=0}^{i} \binom{i}{j}_q a^{i-j} b^j$$

Demonstração. Faremos a demonstração por indução sobre a potência i. Para $i = 1$, temos que:

$$a + b = \binom{1}{0}_q a^1 b^0 + \binom{1}{1}_q a^0 b^1$$

Suponha que $(a+b)^{i-1} = \sum_{j=0}^{i-1} \binom{i-1}{j}_q a^{i-1-j} b^j$. Então:

$$\begin{aligned}
(a+b)^i &= (a+b)\left(\sum_{j=0}^{i-1}\binom{i-1}{j}_q a^{i-1-j}b^j\right)\\
&= \left(\sum_{j=0}^{i-1}\binom{i-1}{j}_q a^{i-j}b^j\right) + \left(\sum_{j=0}^{i-1}\binom{i-1}{j}_q ba^{i-1-j}b^j\right)\\
&= \left(\sum_{j=0}^{i-1}\binom{i-1}{j}_q a^{i-j}b^j\right) + \left(\sum_{j=0}^{i-1}\binom{i-1}{j}_q q^{i-1-j}a^{i-1-j}b^{j+1}\right)\\
&= \binom{i-1}{0}_q a^i b^0 + \left(\sum_{j=1}^{i-1}\left(\binom{i-1}{j}_q + \binom{i-1}{j-1}_q q^{i-j}\right)a^{i-j}b^j\right) + \binom{i-1}{i-1}_q q^0 a^0 b^i\\
&\overset{\text{Lema A.6}}{=} a^i b^0 + \left(\sum_{j=1}^{i-1}\binom{i}{j}_q a^{i-j}b^j\right) + a^0 b^i\\
&= \sum_{j=0}^{i}\binom{i}{j}_q a^{i-j}b^j
\end{aligned}$$

□

Corolário A.8. *Sejam A uma álgebra, q uma n-ésima raiz primitiva da unidade e $a, b \in A$ tais que $ba = qab$. Então temos que:*

$$(a+b)^n = a^n + b^n$$

Demonstração. Usando a proposição A.7, temos que:

$$(a+b)^n = \sum_{j=0}^{n}\binom{n}{j}_q a^{n-j}b^j$$

Mas temos que $\binom{n}{j}_q = 0$ para $1 \leq j \leq n-1$. Portanto:

$$(a+b)^n = a^n + b^n$$

□

B. ÁLGEBRAS E OUTROS RESULTADOS GERAIS

Definição B.1. *Sejam A um $\mathbb{K}$-módulo, $m_A\colon A\otimes A \to A$ e $u_A\colon \mathbb{K}\to A$ morfismos $\mathbb{K}$-lineares. Dizemos que a tripla (A, m_A, u_A) é uma álgebra se os seguintes diagramas comutam:*

$$\begin{tikzcd}
A\otimes A\otimes A \arrow[r, "A\otimes m_A"] \arrow[d, "m_A\otimes A"'] & A\otimes A \arrow[d, "m_A"] \\
A\otimes A \arrow[r, "m_A"] & A
\end{tikzcd}$$

$$\begin{tikzcd}
 & A\otimes A \arrow[dd, "m_A"] & \\
\mathbb{K}\otimes A \arrow[ur, "u_A\otimes A"] \arrow[dr, "\cong"'] & & A\otimes \mathbb{K} \arrow[ul, "A\otimes u_A"'] \arrow[dl, "\cong"] \\
 & A &
\end{tikzcd}$$

Quando não houver ambiguidade, diremos apenas que A é álgebra.

Definição B.2. *Sejam A e B álgebras e $f\colon A\to B$ um morfismo $\mathbb{K}$-linear. Diremos que f é um morfismo de álgebras se os seguintes diagramas comutam:*

$$\begin{tikzcd}
A\otimes A \arrow[r, "f\otimes f"] \arrow[d, "m_A"'] & B\otimes B \arrow[d, "m_B"] \\
A \arrow[r, "f"] & B
\end{tikzcd}$$

$$\begin{tikzcd}
A \arrow[rr, "f"] & & B \\
 & \mathbb{K} \arrow[ul, "u_A"] \arrow[ur, "u_B"'] &
\end{tikzcd}$$

Observação B.3. *A definição acima é equivalente a definição usual de álgebra: $(A, +, \cdot)$ é um anel com unidade e $u\colon \mathbb{K}\to A$ um morfismo de anéis com $u(1) = 1_A$ e $u(\mathbb{K})\subset Z(A)$, onde $Z(A)$ é o centro de A.*

De fato, se A é um anel com unidade e temos um morfismo de anéis $u\colon \mathbb{K}\to A$, então A é um $\mathbb{K}$-módulo por meio de:

$$\lambda a = u(\lambda)a$$

e definindo:

$$\begin{aligned} m_A\colon A\otimes A &\longrightarrow A \\ a\otimes b &\longmapsto a\cdot b \end{aligned}$$

temos que (A, m_A, u) é uma álgebra pela Definição B.1.

Reciprocamente, se (A, m_A, u_A) é uma álgebra pela Definição B.1, então A é um anel por meio de:

$$a\cdot b = m_A(a\otimes b)$$

$$1_A = u_A(1_{\mathbb{K}})$$

e $u_A \colon \mathbb{K} \to A$ *é o morfismo de anéis tal que* $u_A(\mathbb{K}) \subset Z(A)$.

Definição B.4. *Seja* M *um* $\mathbb{K}$*-módulo. Diremos que o par* $(L, \iota \colon M \to L)$ *é uma álgebra tensorial sobre* M *se* L *é uma álgebra,* $\iota \colon M \to L$ *é um morfismo de* $\mathbb{K}$*-módulos e para toda álgebra* A *e todo morfismo de* $\mathbb{K}$*-módulos* $f \colon M \to A$*, existe um único morfismo de álgebras* $f' \colon L \to A$ *tal que o seguinte diagrama comuta:*

$$\begin{tikzcd} & L \arrow[d, dotted, "f"] \\ M \arrow[ur, "\iota"] \arrow[r, "f'"'] & A \end{tikzcd}$$

Teorema B.5. *Para todo* K*-módulo* M*, existe uma única álgebra tensorial* $(L, \iota \colon M \to L)$ *sobre* M*, a menos de isomorfismo.*

Demonstração. Se (L_1, ι_1) e (L_2, ι_2) são álgebras tensoriais sobre M, existem morfismos de álgebras $\varphi \colon L_1 \to L_2$ e $\phi \colon L_2 \to L_1$ tais que os seguintes diagramas comutam:

$$\begin{tikzcd} & L_1 \arrow[d, dotted, "\varphi"] \\ M \arrow[ur, "\iota_1"] \arrow[r, "\iota_2"'] & L_2 \end{tikzcd} \qquad \begin{tikzcd} & L_2 \arrow[d, dotted, "\phi"] \\ M \arrow[ur, "\iota_2"] \arrow[r, "\iota_1"'] & L_1 \end{tikzcd}$$

Logo, os seguintes diagramas comutam:

$$\begin{tikzcd} & L_1 \arrow[d, "\phi \circ \varphi"] \\ M \arrow[ur, "\iota_1"] \arrow[r, "\iota_1"'] & L_1 \end{tikzcd} \qquad \begin{tikzcd} & L_2 \arrow[d, "\varphi \circ \phi"] \\ M \arrow[ur, "\iota_2"] \arrow[r, "\iota_2"'] & L_2 \end{tikzcd}$$

Como as identidades também satisfazem os diagramas acima, pela unicidade temos que $(\phi \circ \varphi) = L_1$ e $(\varphi \circ \phi) = L_2$, o que implica que $L_1 \cong L_2$.

Portanto é suficiente provarmos a existência.

Defina $M_0 = \mathbb{K}$, para cada $i \geq 1$, $M_i = \overbrace{M \otimes \cdots \otimes M}^{i\text{-vezes}}$ e seja L o $\mathbb{K}$-módulo dado por:

$$L = \bigoplus_{i \geq 0} M_i$$

Pela linearidade dos morfismos que usaremos, podemos realizar as verificações para os geradores de M_i. Desta forma, apesar de um elemento geral de M_i ser combinação linear de elementos da forma $x_i = (x_{i,1} \otimes \cdots \otimes x_{i,i})$, utilizaremos estes como os elementos de M_i.

Um elemento arbitrário de L é da forma:

$$x = \sum_{i \geq 0} x_i, \qquad \text{onde } x_i \in M_i \text{ é nulo a menos de um número finito de índices } i$$

Note que $x_0 \in \mathbb{K}$ e $x_i = (x_{i,1} \otimes \cdots \otimes x_{i,i}) \in M_i$ para $i \geq 1$.

Para cada $i, j \geq 0$, defina $\mu_{i,j} \colon M_i \times M_j \to M_{i+j}$ por:

1) se $i \geq 1$ e $j \geq 1$:

$$\mu_{i,j}(x_i, y_j) = x_{i,1} \otimes \cdots \otimes x_{i,i} \otimes y_{j,1} \otimes \cdots \otimes y_{j,j}$$

2) se $i = 0$ e $j \geq 1$:

$$\mu_{0,j}(\lambda, y_j) = \lambda y_j = \lambda y_{j,1} \otimes \cdots \otimes y_{j,j}$$

3) se $i \geq 1$ e $j = 0$:
$$\mu_{i,0}(x_i, \lambda) = \lambda x_i = \lambda x_{i,1} \otimes \cdots \otimes x_{i,i}$$

Claramente temos que $\mu_{i,j}$ é $\mathbb{K}$-bilinear, $\forall i, j \geq 0$.
Além disso, se $x_i \in M_i$, $y_j \in M_j$ e $z_k \in M_k$, temos:

$$\begin{aligned}\mu_{i+j,k}(\mu_{i,j}(x_i, y_j), z_k) &= x_{i,1} \otimes \cdots \otimes x_{i,i} \otimes y_{j,1} \otimes \cdots \otimes y_{j,j} \otimes z_{k,1} \otimes \cdots \otimes z_{k,k} \\ &= \mu_{i,j+k}(x_i, \mu_{j,k}(y_j, z_k))\end{aligned}$$

Os morfismos $m_L \colon L \otimes L \to L$ e $u_L \colon \mathbb{K} \to L$ são definidos da seguinte forma:

$$m_L(x \otimes y) = \sum_{i,j \geq 0} \mu_{i,j}(x_i, y_j)$$

$$u_L(\lambda) = \lambda \in M_0$$

Claramente u_L é morfismo $\mathbb{K}$-linear. Como $\mu_{i,j}$ é $\mathbb{K}$-bilinear para todo $i, j \geq 0$, temos que m_L é morfismo $\mathbb{K}$-bilinear.

Vejamos que os seguintes diagramas comutam:

$$\begin{tikzcd} L \otimes L \otimes L \arrow[r, "L\otimes m_L"] \arrow[d, "m_L\otimes L"'] & L \otimes L \arrow[d, "m_L"] \\ L \otimes L \arrow[r, "m_L"] & L \end{tikzcd}$$

$$\begin{tikzcd} & L \otimes L \arrow[dd, "m_L"] & \\ \mathbb{K} \otimes L \arrow[ur, "u_L\otimes L"] \arrow[dr, "\cong"'] & & L \otimes \mathbb{K} \arrow[ul, "L\otimes u_L"'] \arrow[dl, "\cong"] \\ & L & \end{tikzcd}$$

Sejam $x, y, z \in L$ e $\lambda \in \mathbb{K}$. Então:

$$\begin{aligned}m_L \circ (m_L \otimes L)(x \otimes y \otimes z) &= m_L\Big(\big(\sum_{i,j \geq 0} \mu_{i,j}(x_i, y_j)\big) \otimes z\Big) \\ &= \sum_{i,j,k \geq 0} \mu_{i+j,k}(\mu_{i,j}(x_i, y_j), z_k) \\ &= \sum_{i,j,k \geq 0} \mu_{i,j+k}(x_i, \mu_{j,k}(y_j, z_k)) \\ &= m_L\Big(x, \big(\sum_{j,k \geq 0} \mu_{j,k}(y_j, z_k)\big)\Big) \\ &= m_L \circ (L \otimes m_L)(x \otimes y \otimes z)\end{aligned}$$

$$\begin{aligned}m_L \circ (u_L \otimes L)(\lambda \otimes x) &= m_L(\lambda \otimes x) \\ &= \sum_{i \geq 0} \mu_{0,i}(\lambda, x_i) \\ &= \sum_{i \geq 0} \lambda x_i \\ &= \lambda \sum_{i \geq 0} x_i \\ &= \lambda x\end{aligned}$$

$$\begin{aligned}
m_L \circ (L \otimes u_L)(x \otimes \lambda) &= m_L(x \otimes \lambda)\\
&= \sum_{i \geq 0} \mu_{i,0}(x_i, \lambda)\\
&= \sum_{i \geq 0} \lambda x_i\\
&= \lambda \sum_{i \geq 0} x_i\\
&= \lambda x
\end{aligned}$$

Portanto L é uma álgebra. Definimos ι como:

$$\begin{aligned}
\iota \colon M &\longrightarrow L\\
m &\longmapsto m \in M_1
\end{aligned}$$

Seja A uma álgebra e $f \colon M \to A$ um morfismo $\mathbb{K}$-linear. Definimos f' como:

$$\begin{aligned}
f' \colon L &\longrightarrow A\\
\sum_{i \geq 0} x_i &\longmapsto u_A(x_0) + \sum_{i \geq 1} f(x_{i,1}) \cdots f(x_{i,i})
\end{aligned}$$

Claramente f' é um morfismo $\mathbb{K}$-linear, pois f e u_A são morfismos $\mathbb{K}$-lineares. Vejamos que os seguintes diagramas comutam:

$$\begin{tikzcd}
L \otimes L \arrow[r, "f' \otimes f'"] \arrow[d, "m_L"'] & A \otimes A \arrow[d, "m_A"] \\
L \arrow[r, "f'"] & A
\end{tikzcd}$$

$$\begin{tikzcd}
L \arrow[rr, "f'"] & & A \\
& \mathbb{K} \arrow[ul, "u_L"] \arrow[ur, "u_A"'] &
\end{tikzcd}$$

Sejam $x, y \in L$ e $\lambda \in \mathbb{K}$. Então:

$$\begin{aligned}
f' \circ m_L(x \otimes y) &= f'\big(\sum_{i,j \geq 0} \mu_{i,j}(x_i, y_j)\big)\\
&= f'\big(\mu_{0,0}(x_0, y_0) + \sum_{j \geq 1} \mu_{0,j}(x_0, y_j) + \sum_{i \geq 1} \mu_{i,1}(x_i, y_0) + \sum_{i,j \geq 1} \mu_{i,j}(x_i, y_j)\big)\\
&= u_A(x_0 y_0) + \sum_{j \geq 1} x_0 f(y_{j,1}) \cdots f(y_{j,j}) + \sum_{i \geq 1} y_0 f(x_{i,1}) \cdots f(x_{i,i})\\
&\quad + \sum_{i,j \geq 1} f(x_{i,1}) \cdots f(x_{i,i}) f(y_{j,1}) \cdots f(y_{j,j})
\end{aligned}$$

$$
\begin{aligned}
&m_A \circ (f' \otimes f')(x \otimes y) \\
&\qquad = f'(x)f'(y) \\
&\qquad = \Big(u_A(x_0) + \sum_{i\geq 1} f(x_{i,1})\cdots f(x_{i,i})\Big)\Big(u_A(y_0) + \sum_{j\geq 1} f(y_{j,1})\cdots f(y_{j,j})\Big) \\
&\qquad = u_A(x_0)u_A(y_0) + u_A(x_0)\sum_{j\geq 1} f(y_{j,1})\cdots f(y_{j,j}) + u_A(y_0)\sum_{i\geq 1} f(x_{i,1})\cdots f(x_{i,i}) \\
&\qquad\quad + \sum_{i,j\geq 1} f(x_{i,1})\cdots f(x_{i,i})f(y_{j,1})\cdots f(y_{j,j}) \\
&\qquad = u_A(x_0y_0) + \sum_{j\geq 1} u_A(x_0)f(y_{j,1})\cdots f(y_{j,j}) + \sum_{i\geq 1} u_A(y_0)f(x_{i,1})\cdots f(x_{i,i}) \\
&\qquad\quad + \sum_{i,j\geq 1} f(x_{i,1})\cdots f(x_{i,i})f(y_{j,1})\cdots f(y_{j,j}) \\
&\qquad = u_A(x_0y_0) + \sum_{j\geq 1} x_0u_A(1)f(y_{j,1})\cdots f(y_{j,j}) + \sum_{i\geq 1} y_0u_A(1)f(x_{i,1})\cdots f(x_{i,i}) \\
&\qquad\quad + \sum_{i,j\geq 1} f(x_{i,1})\cdots f(x_{i,i})f(y_{j,1})\cdots f(y_{j,j})
\end{aligned}
$$

$$
\begin{aligned}
f' \circ u_L(\lambda) &= f'(\lambda) \\
&= u_A(\lambda)
\end{aligned}
$$

Portanto f' é morfismo de álgebras. Além disso, como $m = \sum_{i\geq 0} m_i$ com $m_1 = m$ e $m_i = 0$, $\forall i \neq 1$ em L, temos:

$$
\begin{aligned}
f' \circ \iota(m) &= f'(m) \\
&= f(m)
\end{aligned}
$$

Seja $g\colon L \to A$ outro morfismo de álgebras satisfazendo:

$$
\begin{tikzcd}
 & L \arrow[d, dotted, "f"] \\
M \arrow[ur, "\iota"] \arrow[r, "g"'] & A
\end{tikzcd}
$$

Cada elemento de L é da forma $x = \sum_{i\geq 0} x_i =$. Pela definição do produto em L, para $i \geq 1$, podemos reescrever x_i como:

$$x_i = x_{i,1}\cdots x_{i,i}$$

onde $xy = m_L(x \otimes y)$ e cada $x_{i,j} \in M_1$, para todo $1 \leq j \leq i$. Além disso:

$$f(x_{i,j}) = g \circ \iota(x_{i,j}) = g(x_{i,j})$$

Como g é morfismos de álgebras, temos:

$$
\begin{aligned}
g(x_0) &= g \circ u_L(x_0) \\
&= u_A(x_0)
\end{aligned}
$$

$$
\begin{aligned}
g(x_i) &= g(x_{i,1}\cdots x_{i,i}) \\
&= g(x_{i,1})\cdots g(x_{i,i})
\end{aligned}
$$

Logo:

$$\begin{aligned}
f'(x) &= u_A(x_0) + \sum_{i\geq 1} f(x_{i,1}) \cdots f(x_{i,i}) \\
&= g(x_0) + \sum_{i\geq 1} g(x_{i,1}) \cdots g(x_{i,i}) \\
&= \sum_{i\geq 0} g(x_i) \\
&= g\big(\sum_{i\geq 0} x_i\big) \\
&= g(x)
\end{aligned}$$

Portanto $f' = g$ e temos que $(L, \iota\colon M \to L)$ é uma álgebra tensorial sobre M. $\square$

Pelo Teorema B.5, quando $(L, \iota\colon M \to L)$ for a álgebra tensorial sobre M, podemos assumir que M é um $\mathbb{K}$-submódulo de L e que o morfismo $\iota\colon M \to L$ é a inclusão. Assim, diremos apenas que L é a álgebra tensorial sobre M, deixando implícitas as propriedades acima.

Definição B.6. *Sejam A uma álgebra, M um $\mathbb{K}$-módulo e $\vartheta_M\colon A \otimes M \to M$ um morfismo $\mathbb{K}$-linear. Diremos que (M, ϑ_M) é um A-módulo se os seguintes diagramas comutam:*

$$\begin{tikzcd}
A \otimes M \otimes M \arrow[r, "A\otimes m_M"] \arrow[d, "\vartheta_M \otimes M"'] & A \otimes M \arrow[d, "\vartheta_M"] \\
A \otimes M \arrow[r, "\vartheta_M"] & A
\end{tikzcd}$$

$$\begin{tikzcd}
A \otimes M \arrow[rr, "\vartheta_M"] & & A \\
& A \otimes \mathbb{K} \arrow[ul, "A\otimes u_M"] \arrow[ur, "\cong"'] &
\end{tikzcd}$$

Quando não houver ambiguidade, escreveremos apenas que M é um A-módulo.

Proposição B.7. *Sejam A, B álgebras, I um ideal de A e $f\colon A \to B$ tal que $I \subset \ker f$. Então existe um único morfismo de álgebras $\bar{f}\colon A/I \to B$ que faz o seguinte diagrama comutar:*

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\pi_I"'] & & B \\
& A/I \arrow[ur, dotted, "\bar{f}"'] &
\end{tikzcd}$$

onde $\pi_I\colon A \to A/I$ é o morfismo projeção.

Demonstração. Pela propriedade universal de quociente de espaços, temos que existe um único morfismo $\mathbb{K}$-linear que faz o seguinte diagrama comutar:

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\pi_I"'] & & B \\
& A/I \arrow[ur, dotted, "\bar{f}"'] &
\end{tikzcd}$$

Vejamos que $\bar{f}$ é morfismo de álgebras. Sejam $\alpha, \beta \in A$. Então:

$$\begin{aligned}
\bar{f}\left(\left(\alpha+I\right)\left(\beta+I\right)\right) &= \bar{f}\left(\alpha\beta+I\right) \\
&= \bar{f}\circ\pi\left(\alpha\beta\right) \\
&= f\left(\alpha\beta\right) \\
&= f\left(\alpha\right)f\left(\beta\right) \\
&= \bar{f}\circ\pi\left(\alpha\right)\bar{f}\circ\pi\left(\beta\right) \\
&= \bar{f}\left(\alpha+I\right)\bar{f}\left(\beta+I\right)
\end{aligned}$$

e

$$\begin{aligned}
\bar{f}\left(1_{A/I}\right) &= \bar{f}\circ\pi\left(1_A\right) \\
&= f\left(1_A\right) \\
&= 1_B
\end{aligned}$$

Portanto $\bar{f}$ é morfismo de álgebras.
A unicidade segue da propriedade universal do quociente de espaços. $\square$

C. LEMA DO DIAMANTE

Nesta seção apresentaremos os conceitos básicos para entender o Lema do Diamante, com a notação de George Bergman, [6], apenas com uma pequena mudança de notação para ambiguidades. Temos:

- Seja $\mathbb{K}$ um anel comutativo com unidade, X um conjunto, $\langle X \rangle$ o semi grupo livre com unidade sobre X e $\mathbb{K}\langle X \rangle$ a $\mathbb{K}$-álgebra livre associativa sobre X.

- Seja S um conjunto de pares da forma $\sigma = (W_\sigma, f_\sigma)$ com $W_\sigma \in \langle X \rangle$ e $f_\sigma \in \mathbb{K}\langle X \rangle$. Chamaremos S de sistema de reduções.

- Para cada $\sigma \in S$ e $A, B \in \langle X \rangle$, definimos a redução $r_{A\sigma B}$ como o endomorfismo de $\mathbb{K}\langle X \rangle$ tal que:

$$r_{A\sigma B}(AW_\sigma B) = Af_\sigma B \quad \text{e} \quad r_{A\sigma B}(C) = C, \forall AW_\sigma B \neq C \in \langle X \rangle$$

- Dizemos que um elemento $a \in \mathbb{K}\langle X \rangle$ é irredutível (sobre S) se, para qualquer redução r, temos que $r(a) = a$.

- O $\mathbb{K}$-submódulo de $\mathbb{K}\langle X \rangle$ formado pelos elementos irredutíveis será chamado de $\mathbb{K}\langle X \rangle_{irr}$.

- Uma sequência finita de reduções $r_1, ..., r_n$ é dita final em $a \in \mathbb{K}\langle X \rangle$ se:

$$r_n \cdots r_1(a) \in \mathbb{K}\langle X \rangle_{irr}$$

- Uma sequência de reduções $r_1, r_2, ...$ é dita maximal em $a \in \mathbb{K}\langle X \rangle$ se, para cada i:

$$r_i(r_{i-1} \cdots r_1(a)) \neq r_{i-1} \cdots r_1(a)$$

  e

$$\cdots r_2 r_1(a) \in \mathbb{K}\langle X \rangle_{irr}$$

- Diremos que um elemento $a \in \mathbb{K}\langle X \rangle$ é de redução finita se, para toda sequência infinta de reduções $r_1, r_2, ...$, existe $n > 0$ tal que

$$r_i(r_{i-1} \cdots r_1(a)) = r_{i-1} \cdots r_1(a), \forall i \geq n$$

  Note que, se a é de redução finita, toda sequência maximal em a é finita, portanto é final.

- O conjunto de todos os elementos de redução finita forma um $\mathbb{K}$-submódulo de $\mathbb{K}\langle X \rangle$.

- Diremos que um elemento $a \in \mathbb{K}\langle X \rangle$ é de redução única se é de redução finita e toda sequência final de reduções tem a mesma imagem.

- Sejam $A, B, C \in \langle X \rangle$. Diremos que (ABC) é uma ambiguidade se:

1) existem $\sigma, \tau \in S$ tais que $AB = W_\sigma$ e $BC = W_\tau$. Neste caso, a chamamos de ambiguidade de sobreposição. Esta ambiguidade é dita resolúvel se existem composições de reduções r e r' tais que $r(f_\sigma C) = r'(Af_\tau)$;
2) existem $\sigma, \tau \in S$ tais que $ABC = W_\sigma$ e $B = W_\tau$. Neste caso, a chamamos de ambiguidade de inclusão. Esta ambiguidade é dita resolúvel se existem composições de reduções r e r' tais que $r(f_\sigma) = r'(Af_\tau C)$.

- Seja $\leq$ uma ordem parcial de semi grupo em $\langle X \rangle$, ou seja:

$$B < B' \Rightarrow ABC < AB'C, \forall A, C \in \langle X \rangle$$

Diremos que o sistema de reduções S é compatível com $\leq$ se, para todo $\sigma \in S$, f_σ é combinação de elementos de $\langle X \rangle$ menores que W_σ.

- Seja I o ideal bilateral de $\mathbb{K}\langle X \rangle$ gerado por $\{W_\sigma - f_\sigma\}_{\sigma \in S}$ e, para cada $A \in \langle X \rangle$, defina I_A como ideal bilateral de $\mathbb{K}\langle X \rangle$ gerado pelos elementos da forma $B(W_\sigma - f_\sigma)C$, onde $BW_\sigma C < A$.

- Uma ambiguidade (ABC) é resolúvel em relação à $\leq$ se:

1) (sobreposição): $f_\sigma C - Af_\tau \in I_{ABC}$;
2) (inclusão): $f_\sigma - Af_\tau C \in I_{ABC}$.

Teorema C.1 (Lema do Diamante)**.** *[6, Teorema 1.2.] Seja S um sistema de redução para uma álgebra livre associativa $\mathbb{K}\langle X \rangle$, e $\leq$ uma ordem parcial de semi grupo sobre $\langle X \rangle$, compatível com S, com a condição da cadeia descendente. Então são equivalentes:*

1) Todas as ambiguidades de S são resolúveis;

2) Todas as ambiguidades de S são resolúveis em relação à $\leq$;

3) Todos os elementos de $\mathbb{K}\langle X \rangle$ são de redução única;

4) O quociente $R = \mathbb{K}\langle X \rangle / I$ é $\mathbb{K}$-módulo com base dada pelos monômios irredutíveis de $\langle X \rangle$ sobre S.

D. CATEGORIAS MONOIDAIS

Definição D.1. *Seja $\mathcal{C}$ uma categoria. Diremos que $(\mathcal{C}, \otimes, I, \varpi, \omega^l, \omega^r)$ é uma categoria monoidal se:*

$$\otimes \colon \mathcal{C} \times \mathcal{C} \longrightarrow \mathcal{C}$$

é um bifuntor e $I \in \mathcal{C}$ é tal que, $\forall A, B, C \in \mathcal{C}$, temos os seguintes isomorfismos naturais:

$$\varpi = \varpi_{A,B,C} \colon A \otimes (B \otimes C) \longrightarrow (A \otimes B) \otimes C$$

$$\omega^l_A \colon I \otimes A \longrightarrow A$$

$$\omega^r_A \colon A \otimes I \longrightarrow A$$

e os seguintes diagramas comutam, $\forall A, B, C, D \in \mathcal{C}$:

$$\begin{tikzcd}
A \otimes (B \otimes (C \otimes D)) \arrow[r, "\varpi"] \arrow[d, "A\otimes\varpi"'] & (A \otimes B) \otimes (C \otimes D) \arrow[r, "\varpi"] & ((A \otimes B) \otimes C) \otimes D \\
A \otimes ((B \otimes C) \otimes D) \arrow[rr, "\varpi"] & & (A \otimes (B \otimes C)) \otimes D \arrow[u, "\varpi\otimes D"']
\end{tikzcd}$$

$$\begin{tikzcd}
I \otimes (B \otimes C) \arrow[rr, "\varpi"] \arrow[dr, "\omega^l_{B\otimes C}"'] & & (I \otimes B) \otimes C \arrow[dl, "\omega^l_B \otimes C"] \\
& B \otimes C &
\end{tikzcd}
\qquad
\begin{tikzcd}
A \otimes (B \otimes I) \arrow[rr, "\varpi"] \arrow[dr, "A\otimes\omega^r_B"'] & & (A \otimes B) \otimes I \arrow[dl, "\omega^r_{A\otimes B}"] \\
& A \otimes B &
\end{tikzcd}$$

Definição D.2. *Sejam $(\mathcal{C}, \otimes, I, \varpi, \omega^l, \omega^r)$ e $(\mathcal{C}', \otimes', I', \varpi', \omega'^l, \omega'^r)$ categorias monoidais. Um funtor monoidal fraco entre estas categorias:*

$$T \colon (\mathcal{C}, \otimes, I, \varpi, \omega^l, \omega^r) \longrightarrow (\mathcal{C}', \otimes', I', \varpi', \omega'^l, \omega'^r)$$

é um funtor $T \colon \mathcal{C} \to \mathcal{C}'$ tal que, $\forall A, B, C \in \mathcal{C}$, existem morfismos:

$$\xi \colon T(A) \otimes' T(B) \longrightarrow T(A \otimes B)$$

e

$$\xi_0 \colon I' \longrightarrow T(I)$$

que satisfazem os seguintes diagramas:

$$\begin{tikzcd}
T(A) \otimes' (T(B) \otimes' T(C)) \arrow[r, "\varpi'"] \arrow[d, "T(A)\otimes'\xi"'] & (T(A) \otimes' T(B)) \otimes' T(C) \arrow[d, "\xi\otimes' T(C)"] \\
T(A) \otimes' T(B \otimes C) \arrow[d, "\xi"'] & T(A \otimes B) \otimes' T(C) \arrow[d, "\xi"] \\
T(A \otimes (B \otimes C)) \arrow[r, "T(\varpi)"] & T((A \otimes B) \otimes C)
\end{tikzcd}$$

$$\begin{tikzcd}
I' \otimes' T(A) \arrow[r, "\omega'^l_{T(A)}"] \arrow[d, "\xi_0\otimes' T(A)"'] & T(A) \\
T(I) \otimes' T(A) \arrow[r, "\xi"] & T(I \otimes A) \arrow[u, "T(\omega^l_A)"']
\end{tikzcd}
\qquad
\begin{tikzcd}
T(A) \otimes' I' \arrow[r, "\omega'^r_{T(A)}"] \arrow[d, "T(A)\otimes'\xi_0"'] & T(A) \\
T(A) \otimes' T(I) \arrow[r, "\xi"] & T(A \otimes I) \arrow[u, "T(\omega^r_A)"']
\end{tikzcd}$$

Exemplo D.3. *A categoria dos $\mathbb{K}$-módulos é uma categoria monoidal com o produto tensorial e isomorfismos canônicos:*

$$\begin{aligned} \varpi\colon M \otimes (N \otimes S) &\longrightarrow (M \otimes N) \otimes S \\ m \otimes n \otimes s &\longmapsto m \otimes n \otimes s \end{aligned}$$

$$\begin{aligned} \omega^l_M\colon \mathbb{K} \otimes M &\longrightarrow M \\ \lambda \otimes m &\longmapsto \lambda m \end{aligned}$$

e

$$\begin{aligned} \omega^r_M\colon M \otimes \mathbb{K} &\longrightarrow M \\ m \otimes \lambda &\longmapsto \lambda m \end{aligned}$$

BIBLIOGRAFIA

[1] J. BICHON, Galois and Bigalois Objects Over Monomial Non-Semisimple Hopf Algebras, J. Algebra Appl. (2006), 653-680.

[2] P. SCHAUENBURG, Hopf Bigalois Extensions, Comm. Algebra 24(12) (1996), 3797-3825.

[3] P. SCHAUENBURG, Hopf-Galois and Bi-Galois Extensions, Fields Inst. Commun. 43 AMS (2004) 469-515.

[4] S. MONTGOMERY, Hopf Algebras and Their Actions on Rings (Amer. Math. Soc., Providence, 1993).

[5] M. SWEEDLER, Cohomology of Algebras Over Hopf Algebras, Transactions of the American Mathematical Society Vol. 133, No. 1 (1968), 205-239

[6] G. M. BERGMAN, The Diamond Lemma for Ring Theory, Adv. Math. 29 (1978), 178-218.

[7] X.-W. CHEN, H.-L. HUANG, Y. YE e P. ZHANG, Monomial Hopf algebras, J. Algebra 275 (2004), 212-232.

[8] G. KARPILOVSKY, Projective Representations of Finite Groups (Marcel Dekker, 1985).

[9] C. GALINDO, M. MEDINA, On the Classification of Galois Objects for Finite Groups, Communications in Algebra Vol. 40, Issue 7, (2012), 2577-2595

[10] E. J. TAFT, The Order of the Antipode of Finite-Dimensional Hopf Algebra, Proc. Nat. Acad. Sci. USA Vol. 68, No. 11 (1971), 2631-2633

[11] P. J. MCCARTHY, Algebraic Extensions of Fields (Dover Publications, 1991).

[12] S. MAC LANE, Categories for the Working Mathematician (Springer, 1998).

[13] D. E. RADFORD, Hopf Algebras, (World Scientific, 2012).

[14] D. G. NORTHCOTT, Multilinear Algebra, (Cambridge University Press, 1984).

[15] T. MASZCZYK, Galois Structures, 2008. Disponível em: `http://toknotes.mimuw.edu.pl/sem7/files/Maszczyk_gs.pdf`. Acessado em 28 de janeiro de 2014.